INFORMATION AND COMPUTATION 123, 210–223 (1995)

The Availability of Quorum Systems

DAVID PELEG* AND AVISHAI WOOL

Department of Applied Mathematics and Computer Science, The Weizmann Institute, Rehovot 76100, Israel
E-mail: {peleg, yash}@wisdom.weizmann.ac.il

A *quorum system* is a collection of sets (quorums) every two of which intersect. Quorum systems have been used for many applications in the area of distributed systems, including mutual exclusion, data replication, and dissemination of information. In this paper we study the failure probabilities of quorum systems and in particular of non-dominated coteries (NDC). We characterize NDC's in terms of the failure probability, and prove that any NDC has availability that falls between that of a singleton and a majority consensus. We show conditions for weighted voting schemes to provide asymptotically high availability, and we analyze the availability of several other known quorum systems.

1. INTRODUCTION

1.1. *Motivation*

Quorum systems serve as a basic tool providing a uniform and reliable way to achieve coordination between processors in a distributed system. Quorum systems are defined as follows. A *set system* is a collection of sets $\mathcal{S} = \{S_1, ..., S_m\}$ over an underlying universe $U = \{u_1, ..., u_n\}$. A set system is said to satisfy the *intersection property*, if every two sets $S, R \in \mathcal{S}$ have a non-empty intersection. Set systems with the intersection property are known as *quorum systems*, and the sets in such a system are called quorums.

Quorum systems have been used in the study of distributed control and management problems such as *mutual exclusion* (cf. [Ray86]), *data replication protocols* (cf. [DGS85, Her84]), *name servers* (cf. [MV88]), *selective dissemination of information* (cf. [YG94]), and *distributed access control and signatures* (cf. [NW95]).

A protocol template based on quorum systems works as follows. In order to perform some action (e.g., update the database, enter a critical section), the user selects a quorum and *accesses all its elements*. The intersection property then guarantees that the user will have a consistent view of the current state of the system. For example, if all the members of a certain quorum give the user permission to enter the critical section, then any other user trying to enter the critical section before the first user has exited (and released the permission-granting quorum from its lock) will be refused permission by at least one member of any quorum it chooses to access.

* Supported in part by a Walter and Elise Haas Career Development Award and by a grant from the Israeli Basic Research Foundation.

1.2. *Related Work*

The first distributed control protocols using quorum systems [Tho79, Gif79] use *voting* to define the quorums. Each processor has a number of votes, and a quorum is any set of processors with a combined number of votes exceeding half of the system's total number of votes. The simple majority system is the most obvious voting system.

Alternative protocols based on quorum systems (rather than on voting) appear in [Mae85] (using finite projective planes), [AE91] (the Tree system), [CAA90, KRS93] (using a grid), and [Kum91, KC91, RT91, RST92] (hierarchical systems). The triangular system is due to [Lov73, EL75]. The Wheel system appears in [MP92a]. The class of "Crumbling Wall" coteries appears in [PW95].

The first paper to explicitly consider mutual exclusion protocols in the context of intersecting set systems is [GB85]. In this work, the term *coterie* and the concept of *domination* are introduced. Several basic properties of dominated and non-dominated coteries and of the class of non-dominated coteries (denoted NDC) are proved.

The *fault-tolerance* properties of quorum-based mutual exclusion protocols are introduced in [BG86] and studied further in [Coh93]. The fault tolerance of a quorum system is measured by the maximal number of processors that can fail before all the quorums are "hit," in the worst possible configuration of failures. A quorum is "hit" once at least one of its members has failed.

The failure probability F_p, or equivalent notions such as reliability or availability, are well known in reliability theory [BP75]. In [BG87] the availability of coteries is studied. It is shown that in a complete network the optimal availability quorum system is the majority (Maj) coterie if $p < 1/2$. The case when the elements fail with different probabilities p_i, all less than 1/2, is addressed in [SB94]. The availability of k-coteries is studied in [KFYA93].

A characterization of non-dominated coteries in terms of boolean functions appears in [IK93, BI95]. The issue of balancing the work load in quorum systems is studied in

0890-5401/95 $12.00

[MP92b, HMP95]. The load and capacity of quorum systems, and their trade-offs with the availability, appear in [NW94].

1.3. *Contents*

In this paper, we consider the fault-tolerance properties of coteries, and of mutual exclusion protocols based on them. It is assumed that individual processors are subject to occasional failures, and the focus of this study is the question: "given a quorum system $\mathcal{S}$, what is the probability of a system failure, i.e., of being left with no functioning quorum available?". We assume the common model in which each element fails independently of all other elements, with a uniform probability p. Under this assumption, we examine the properties of the failure probability, denoted by $F_p(\mathcal{S})$. Formally, let X denote the random set of failed elements in the universe U. Then $F_p(\mathcal{S}) = \mathbb{P}(\forall S \in \mathcal{S}, S \cap X \neq \varnothing)$.

As will be shown in the sequel, it turns out that the property of *non-domination* has a strong effect on the failure probability $F_p(\mathcal{S})$. It is known that the NDCs are "the most available" quorum systems (e.g., [BG86, INK92]). Over the NDCs, the behavior of the failure probability F_p depends on the exact value of p. We show that for any $\mathcal{S} \in$ NDC, $F_p(\mathcal{S})$ is symmetric, i.e., $F_p(\mathcal{S}) = 1 - F_{1-p}(\mathcal{S})$. In particular, $F_{1/2}(\mathcal{S}) = 1/2$ for any $\mathcal{S} \in$ NDC. The converse is also true, i.e., if $F_{1/2}(\mathcal{S}) = 1/2$ then $\mathcal{S} \in$ NDC. As a consequence, we also obtain a new proof for the lower bound of [Erd63] on the number of quorums in an NDC.

We then consider the quorum system constructions that have the extremal failure probabilities. We show that for $0 < p < 1/2$, the least available NDC (highest $F_p(\mathcal{S})$) is the "monarchy" (the singleton system Sngl). By the same proof we get almost for free a new proof for the result of [BG87], that the most available NDC is the "democracy" (the majority system Maj). By the above mentioned symmetry of F_p, when $1/2 < p < 1$ the situation is reversed. This means that if the elements are fail-prone, with an individual failure probability greater than 1/2, the situation is uninteresting; the best strategy is just to pick a single centralized "king." We have very recently learned that the optimality of the monarchy when $p > 1/2$ has been obtained independently by Diks *et al.* [DKK⁺94]. We also show that if we require all the elements to appear in some quorum, then the Wheel system of [MP92a] replaces the singleton as the extremal system.

When the elements are not fail-prone, with $0 < p < 1/2$, then it is interesting to investigate other constructions. This is since the NDC with the best availability, the majority system Maj, has some undesirable properties (e.g., very large quorums). We analyze the availability of several constructions that appear in the literature. Our analysis emphasizes the asymptotic behavior of $F_p(\mathcal{S})$, as the construction scales up with the universe size n. A desirable property of a quorum system construction is that its failure probability is "*Condorcet*." By this we mean that $F_p(\mathcal{S}) \to 0$ as $n \to \infty$ when $0 < p < 1/2$, (and $F_p(\mathcal{S}) \to 1$ as $n \to \infty$ when $1/2 < p < 1$). The Condorcet Jury Theorem [Con], translated to our terminology, states that the majority NDC has this property. We show that several other constructions also have Condorcet failure probabilities (e.g., the constructions of [EL75, AE91]), while others still (e.g., [Lov73]) have a nonzero limit function when $p < 1/2$. Moreover, as shown in [RST92, KC91], the *finite projective plane* construction [Mae85] and *grid* construction [CAA90] have failure probabilities tending to 1 for *all* values $0 < p < 1$.

A simple and popular method of NDC construction is that of weighted voting. When all the votes are equal, this gives the simple majority system. We show that if the ratio between the total weight and the maximal weight tends to infinity as $n \to \infty$ then $F_p(\mathcal{S})$ is Condorcet. Alternatively, if the ratio between the sum of squared weights and the total weight squared tends to 0, then $F_p(\mathcal{S})$ is Condorcet.

From a practical point of view, we can see that $F_p(\mathcal{S})$ gives us a yardstick for comparing different quorum systems, and distributed protocols based upon them, which is especially meaningful when the number of processors is large. In particular, our analysis leads to the following conclusions, on the basis of availability considerations: it is preferable to avoid finite projective plane or grid systems on large scale systems; while the majority NDC has the highest availability, there are NDCs which have comparable availability but are not as costly; when using voting, and all the processors have identical availability, it is preferable to have a "flat" distribution of votes.

The organization of this paper is as follows. In Section 2, we present some basic definitions, and a precise definition of our model. In Section 3, we start the analysis of $F_p(\mathcal{S})$ of NDCs by proving the symmetry theorem and some of its consequences. In Section 4, we prove that the majority and singleton are the extremal NDCs in terms of $F_p(\mathcal{S})$. In Section 5, we analyze several known constructions. In Section 6, we present the conditions for having a Condorcet failure probability in a voting system.

A preliminary version of this paper can be found in [PW93].

2. PRELIMINARIES

2.1. *Definitions and Notation*

Let us first define the basic terminology used later on.

Definition 2.1. A *Set System* $\mathcal{S} = \{S_1, ..., S_m\}$ is a collection of subsets $S_i \subseteq U$ of a finite universe U. A *Quorum System* is a set system $\mathcal{S}$ that has the *Intersection property*: $S \cap R \neq \varnothing$ for all $S, R \in \mathcal{S}$.

Alternatively, quorum systems are known as *intersecting set systems* or as *intersecting hypergraphs*. The sets of the system are called *quorums* (or *edges*, when using the hypergraph terminology).

DEFINITION 2.2. A *Coterie* is a quorum system $\mathcal{S}$ that has the *Minimality property*: there are no $S, R \in \mathcal{S}$, $S \subset R$.

DEFINITION 2.3. Let $\mathcal{R}$, $\mathcal{S}$ be coteries (over the same universe U). $\mathcal{R}$ *dominates* $\mathcal{S}$ (denoted $\mathcal{R} \succ \mathcal{S}$) if $\mathcal{R} \neq \mathcal{S}$ and for each $S \in \mathcal{S}$ there is $R \in \mathcal{R}$ such that $R \subseteq S$.

DEFINITION 2.4. A coterie $\mathcal{S}$ is *dominated* if there exists a coterie $\mathcal{R}$ such that $\mathcal{R} \succ \mathcal{S}$. If no such coterie exists then $\mathcal{S}$ is *non-dominated* (ND). Let NDC denote the class of all ND coteries.

DEFINITION 2.5. A set T is a *transversal* of a set system $\mathcal{S}$ if for every $S \in \mathcal{S}$, $T \cap S \neq \varnothing$.

We use the following notation. The number of elements in the underlying universe is denoted by $n = |U|$. The number of sets (quorums) in the set system $\mathcal{S}$ is denoted by $m(\mathcal{S})$. The cardinality of the smallest quorum in $\mathcal{S}$ is denoted by $c(\mathcal{S}) = \min\{|S| : S \in \mathcal{S}\}$.

Notation. Let $\mathcal{U}^{(i)} = \{X \subseteq U : |X| = i\}$, the collection of sets of size i for $0 \leqslant i \leqslant n$.

DEFINITION 2.6. Let $\mathcal{A}_i^{\mathcal{S}}$ denote the set of size-i transversals of $\mathcal{S}$, i.e., the collection of sets of size i that hit all the quorums of S, for $0 \leqslant i \leqslant n$,

$$\mathcal{A}_i^{\mathcal{S}} = \{X \in \mathcal{U}^{(i)} : \forall S \in \mathcal{S}, S \cap X \neq \varnothing\}.$$

Let us illustrate the concept of quorum systems by giving three examples, the *singleton* system, the *majority* system, and the *wheel* system. These examples play an important role in the results of this paper.

The singleton system, denoted by Sngl, is the set system $\text{Sngl} = \{\{u\}\}$.

If the universe size $n = |U|$ is odd, then the majority system, denoted by Maj, is the collection of all sets of $(n+1)/2$ elements. If n is even, we pick an element $u \in U$ and define Maj to be the collection of all sets of size $n/2$ *that do not include u*. In other words, we ignore the element u and use the Maj system on the odd sized universe $U \backslash \{u\}$.

The Wheel contains $n-1$ "spoke" quorums of the form $\{1, i\}$ for $i = 2, ..., n$, and one "rim" quorum, $\{2, ..., n\}$.

It is easy to see that Sngl $\in$ NDC and that Wheel $\in$ NDC. Also, our definition of the majority system ensures that Maj $\in$ NDC for all n (note that when n is even, the everyday notion of taking sets of size $n/2 + 1$ gives a dominated coterie).

2.2. *Basic Theorems*

The following theorems regarding coterie domination will be our basic tools throughout this work.

LEMMA 2.7 [GB85]. *Let $\mathcal{S} \in$ NDC and let T be a transversal of $\mathcal{S}$. Then there exists a quorum $S \in \mathcal{S}$ s.t. $S \subseteq T$.*

LEMMA 2.8 [IK93]. *Let $\mathcal{S}$ be a coterie. Then $\mathcal{S} \in$ NDC iff for all $X \subseteq U$, exactly one of X and $U \backslash X$ is a transversal of $\mathcal{S}$.*

THEOREM 2.9 [GB85]. *Let $\mathcal{S}$, $\mathcal{R}$ be coteries. Then $\mathcal{R} \succ \mathcal{S}$ iff there exists a quorum $R_0 \in \mathcal{R}$ such that R_0 is a transversal of $\mathcal{S}$ and $R_0 \nsupseteq S$ for every $S \in \mathcal{S}$.*

LEMMA 2.10. *Let $\mathcal{S} \in$ NDC be given. Then $\mathcal{A}_i^{\mathcal{S}}$ is an intersecting hypergraph in $\mathcal{U}^{(i)}$ for $0 \leqslant i \leqslant n$.*

Proof. Consider two sets $X_1, X_2 \in \mathcal{A}_i^{\mathcal{S}}$ for some i. Then X_1 and X_2 are transversals of $\mathcal{S}$, so from Lemma 2.7 there exist quorums $S_1, S_2 \in \mathcal{S}$ such that $S_1 \subseteq X_1$ and $S_2 \subseteq X_2$. From the Intersection property of $\mathcal{S}$, we have that $X_1 \cap X_2 \neq \varnothing$. Therefore $\mathcal{A}_i^{\mathcal{S}}$ is an intersecting hypergraph in $\mathcal{U}^{(i)}$. ∎

The following is the celebrated Erdős–Ko–Rado theorem [EKR61] (cf. [Bol86]), also known as the Sunflower Theorem.

THEOREM 2.11 (Sunflower) [EKR61]. *Consider a universe U of size n. Let $2 \leqslant i < n/2$ and let $\mathcal{A} \subseteq \mathcal{U}^{(i)}$ be an intersecting hypergraph. Then $|\mathcal{A}| \leqslant \binom{n-1}{i-1}$, with equality iff $\mathcal{A} = \{X \in \mathcal{U}^{(i)} : u \in X\}$ for some $u \in U$.*

Remark. The theorem is trivially true for $i = 1$ as well.

We now introduce some definitions and results from [Kar68] that are used in Section 4. The results are not presented in their most general formulation, but rather in a form suited to their intended use in our proof.

DEFINITION 2.12 (Total Positivity). A real function (kernel) $K(x, y)$ of two variables ranging over linearly ordered sets X and Y, respectively, is called *totally positive of order r* (abbreviated TP_r) if for all $x_1 < \cdots < x_\ell$, $y_1 < \cdots < y_\ell$, $x_i \in X$, $y_j \in Y$, $1 \leqslant \ell \leqslant r$ the following inequality holds:

$$\begin{vmatrix} K(x_1, y_1) & K(x_1, y_2) & \cdots & K(x_1, y_\ell) \\ K(x_2, y_1) & K(x_2, y_2) & \cdots & K(x_2, y_\ell) \\ \vdots & \vdots & & \vdots \\ K(x_\ell, y_1) & K(x_\ell, y_2) & \cdots & K(x_\ell, y_\ell) \end{vmatrix} \geqslant 0.$$

A kernel K is said to be *totally positive* (TP) if it is TP_r for all values of r.

DEFINITION 2.13 (Sign Changes). Let $f(t)$ be defined in I, where I is an ordered set of the real line. Let $S^-[x_1, x_2, ..., x_\ell]$ denote the number of sign changes of the indicated sequence, zero terms discarded. Define

$$S^-(f) = \sup S^-[f(t_1), f(t_2), ..., f(t_\ell)]$$

where the supremum is over all sets $t_1 < \cdots < t_\ell$ ($t_i \in I$), where ℓ is arbitrary but finite. If $f \equiv 0$ then define $S^-(f) = -1$.

Let I be an finite ordered set of the real line, and let f be defined on I. Let X be a closed interval. Let $K(x, i)$ be defined on $X \times I$. Consider the transformation T (of f) defined by

$$(Tf)(x) = \sum_{i \in I} K(x, i)\, f(i).$$

THEOREM 2.14 (Variation Diminishing Property) [Kar68]. *If a kernel K is TP and $g(x) = (Tf)(x)$ then $S^-(g) \leqslant S^-(f)$. Furthermore, the values of the functions f and g exhibit the same sequence of signs when their respective arguments traverse the domain of definition from left to right.*

Fact 2.15. The kernel $K(p, i) = p^i(1-p)^{n-i}$ defined over $[0, 1] \times \{0, ..., n\}$ is *TP*.

2.3. *The Probabilistic Failure Model*

We use a simple probabilistic model of the failures in the system. We assume that the elements (processors) fail independently with a fixed uniform probability p. We assume that the failures are *transient*. We assume also that the failures are *crash* failures, and that they are *detectable*. In other words, we do not consider "lying" processors (Byzantine failures), or asynchronous communication with unbounded message delay.

The points of our probability space are called *configurations*. A configuration is a set $X \subseteq U$, where all the elements of X have failed and all other elements have not.

Notation. We use $q = 1 - p$ to denote the probability of an element survival.

In this failure model with probability p, the following events can be defined.

DEFINITION 2.16 (Quorum Failure). For every quorum $S \in \mathcal{S}$ let $\mathcal{E}_S$ be the event that S is *hit*, i.e., at least one element $x \in S$ has failed (or, $S \cap X \neq \emptyset$).

Using this definition, the failure probability of a quorum $S \in \mathcal{S}$ is $\mathbb{P}(\mathcal{E}_S) = 1 - q^{|S|}$.

DEFINITION 2.17 (System Failure). Let *fail*($\mathcal{S}$) be the event that all the quorums $S \in \mathcal{S}$ were hit, i.e., *fail*$(\mathcal{S}) = \bigcap_{S \in \mathcal{S}} \mathcal{E}_S$.

Note that the event *fail*($\mathcal{S}$) consists of precisely the transversal configurations of $\mathcal{S}$, i.e.,

$$fail(\mathcal{S}) = \{X \subseteq U : X \text{ is a transversal of } \mathcal{S}\}.$$

Now we can define the focus of this work, which is the global system failure probability of a quorum system $\mathcal{S}$, as follows.

DEFINITION 2.18.

$$F_p(\mathcal{S}) = \mathbb{P}(fail(\mathcal{S})) = \mathbb{P}\left(\bigcap_{S \in \mathcal{S}} \mathcal{E}_S\right).$$

Fact 2.19. For any set system $\mathcal{S}$, $F_0(\mathcal{S}) = 0$ and $F_1(\mathcal{S}) = 1$. ∎

Given a quorum system $\mathcal{S}$, We find it useful to count the transversals according to their cardinalities using Definition 2.6, as follows.

DEFINITION 2.20. Let $a_i^{\mathcal{S}} = |\mathcal{A}_i^{\mathcal{S}}|$, the number of i-sized transversals of $\mathcal{S}$. The vector $a^{\mathcal{S}} = (a_0^{\mathcal{S}}, ..., a_n^{\mathcal{S}})$ is called the *availability profile* of $\mathcal{S}$.

Using the availability profile we can write an explicit expression for the failure probability $F_p(\mathcal{S})$.

LEMMA 2.21. $F_p(\mathcal{S}) = \sum_{i=0}^{n} a_i^{\mathcal{S}} p^i q^{n-i}$.

When we consider the asymptotic behavior of $F_p(\mathcal{S}_n)$ for a sequence $\mathcal{S}_n$ of NDCs over a universe with an increasing size n, we find that for many constructions it is similar to the behavior described by the Condorcet Jury Theorem [Con]. Therefore it is useful to have the following definition.

DEFINITION 2.22. A parameterized family of functions $g_p(n)$: $\mathbb{N} \to [0, 1]$, for $p \in [0, 1]$, is said to be *Condorcet* iff

$$\lim_{n \to \infty} g_p(n) = \begin{cases} 0, & p < \frac{1}{2}, \\ 1, & p > \frac{1}{2}, \end{cases} \quad \text{and} \quad g_{1/2}(n) = \tfrac{1}{2} \text{ for all } n.$$

If we generalize our model and allow different probabilities p_i for the elements, then we enter the domain of reliability theory. Below we introduce a more general definition of the failure probability, and a basic theorem which will be useful to us. The definitions are rephrased using our terminology. A good reference to reliability theory is [BP75].

DEFINITION 2.23. For a quorum system $\mathcal{S}$, let $\mathcal{A} = \{A \subseteq U : A \cap S \neq \emptyset \text{ for all } S \in \mathcal{S}\}$ be the collection of transversals of $\mathcal{S}$. Let $\mathbf{p} = (p_1, ..., p_n)$ denote the failure probabilities of the elements. Then

$$h_{\mathcal{S}}(\mathbf{p}) = \sum_{A \in \mathcal{A}} \prod_{i \in A} p_i \prod_{i \notin A} (1 - p_i)$$

is the failure probability of $\mathcal{S}$.

THEOREM 2.24 [BP75]. *Let a quorum system $\mathcal{S}$ be given. Then $h_{\mathcal{S}}(\mathbf{p})$ is strictly increasing in p_i for every non-redundant element i (i.e., $i \in S$ for some minimal $S \in \mathcal{S}$).*

If we return to the case of equal failure probabilities, then $h_{\mathcal{S}}(p, p, ..., p) = F_p(\mathcal{S})$. Since every (non-empty) quorum system has some element that is not redundant, we obtain the following corollary of Theorem 2.24.

COROLLARY 2.25. *$F_p(\mathcal{S})$ is strictly increasing with p for every quorum system $\mathcal{S}$.*

3. AVAILABILITY ANALYSIS OF NDCs

3.1. *The Symmetry of $F_p(\mathcal{S})$*

Our purpose in this section is to prove a symmetry theorem for the failure probability of ND coteries. We show that for any given $\mathcal{S} \in \text{NDC}$, the function $F_p(\mathcal{S})$: $[0, 1] \rightarrow [0, 1]$ (as a function of p) has rotational symmetry around 1/2.

The following lemma shows a property of the availability profile of ND coteries, which is the combinatorial basis of the symmetry theorem.

LEMMA 3.1. *Let $\mathcal{S} \in \text{NDC}$ be given. Then $a_i^{\mathcal{S}} + a_{n-i}^{\mathcal{S}} = \binom{n}{i}$ for $0 \leqslant i \leqslant n$.*

Proof. Let $\mathcal{B}_i^{\mathcal{S}} = \mathcal{U}^{(i)} \setminus \mathcal{A}_i^{\mathcal{S}}$, the set of all configurations of size i that do not hit some $S \in \mathcal{S}$, and let $b_i^{\mathcal{S}} = |\mathcal{B}_i^{\mathcal{S}}|$. Clearly $a_i^{\mathcal{S}} + b_i^{\mathcal{S}} = \binom{n}{i}$. Therefore it suffices to show that $b_i^{\mathcal{S}} = a_{n-i}^{\mathcal{S}}$. Consider a configuration $X \in \mathcal{U}^{(i)}$ and let $\bar{X} = U \setminus X$. We claim that $X \in \mathcal{B}_i^{\mathcal{S}} \Leftrightarrow \bar{X} \in \mathcal{A}_{n-i}^{\mathcal{S}}$. It is clear that $|\bar{X}| = n - i$, so either $\bar{X} \in \mathcal{A}_{n-i}^{\mathcal{S}}$ or $\bar{X} \in \mathcal{B}_{n-i}^{\mathcal{S}}$. It therefore remains to prove that $\bar{X}$ is a transversal of $\mathcal{S}$ iff X is not, but this follows immediately from Lemma 2.8. Thus there is a one-to-one correspondence between $\mathcal{B}_i^{\mathcal{S}}$ and $\mathcal{A}_{n-i}^{\mathcal{S}}$, so $b_i^{\mathcal{S}} = a_{n-i}^{\mathcal{S}}$. ∎

The following is an easily deduced corollary of Lemma 3.1 when the universe U has an even size.

COROLLARY 3.2. *Let $\mathcal{S} \in \text{NDC}$. If $n = 2t$ then $a_t^{\mathcal{S}} = \frac{1}{2}\binom{n}{t} = \binom{n-1}{t-1}$.*

Now we can prove the symmetry theorem of $F_p(\mathcal{S})$ for NDCs.

THEOREM 3.3 (Symmetry). *For any $\mathcal{S} \in \text{NDC}$, $F_p(\mathcal{S}) + F_{1-p}(\mathcal{S}) = 1$.*

Proof. From Lemma 2.21 and Lemma 3.1, and some standard manipulations, we get

$$
\begin{aligned}
F_p(\mathcal{S}) + F_{1-p}(\mathcal{S}) &= \sum_{i=0}^{n} a_i^{\mathcal{S}} p^i (1-p)^{n-i} + \sum_{i=0}^{n} a_i^{\mathcal{S}} (1-p)^i p^{n-i} \\
&= \sum_{i=0}^{n} (a_i^{\mathcal{S}} + a_{n-i}^{\mathcal{S}})(1-p)^i p^{n-i} \\
&= \sum_{i=0}^{n} \binom{n}{i} (1-p)^i p^{n-i} = 1. \quad ∎
\end{aligned}
$$

Plugging $p = 1/2$ into the symmetry theorem we get the following corollary.

COROLLARY 3.4. *For any $\mathcal{S} \in \text{NDC}$, $F_{1/2}(\mathcal{S}) = 1/2$.*

Remark. An alternative proof for Theorem 3.3 has been suggested to us [Hol93]. This proof is based on the fact that the failure probability of an ND coterie can be viewed as the *multi-linear extension* (MLE) of a constant-sum game. Consequently, Theorem X.2.6 of [Owe82, pp. 201–202] can be used to obtain the claim. Theorem 3.3 can also be derived from the self-duality of NDCs; cf. [IK93].

3.2. *Conditions for Non-domination*

We now present two consequences of the symmetry theorem. The first is a characterization of NDCs in terms of the failure probability $F_{1/2}$. This characterization (Corollary 3.9) gives another method of proving coterie non-domination which is sometimes easier than a direct proof. The second consequence we obtain from the symmetry theorem is a lower bound on $m(\mathcal{S})$, the number of quorums in a system $\mathcal{S} \in \text{NDC}$, in terms of $c(\mathcal{S})$, the cardinality of the smallest quorum.

The following lemma of [INK92] shows that NDCs are "better" (i.e., have higher availability) than dominated coteries.

LEMMA 3.5 [INK92]. *Let $\mathcal{S}$, $\mathcal{R}$ be coteries such that $\mathcal{R} \succ \mathcal{S}$, and let $0 < p < 1$. Then $F_p(\mathcal{R}) \leqslant F_p(\mathcal{S})$.*

We improve this result slightly by showing that NDCs are strictly better. This is necessary for the proof of Corollary 3.9.

LEMMA 3.6. *Let $\mathcal{S}$, $\mathcal{R}$ be coteries such that $\mathcal{R} \succ \mathcal{S}$, and let $0 < p < 1$. Then $F_p(\mathcal{R}) < F_p(\mathcal{S})$.*

Proof. We show a non-zero probability configuration that is in *fail*($\mathcal{S}$) but not in *fail*($\mathcal{R}$). Consider a quorum $R_0 \in \mathcal{R}$ such that R_0 is a transversal of $\mathcal{S}$ and R_0 is not a superset of any $S \in \mathcal{S}$. The existence of such an R_0 is guaranteed by Theorem 2.9. We claim that $\bar{R}_0 = U \setminus R_0$ is also a transversal of $\mathcal{S}$. To see this, assume to the contrary that there exists a quorum $S \in \mathcal{S}$ such that $\bar{R}_0 \cap S = \varnothing$. Then $S \subseteq R_0$, contradiction to the properties of R_0.

Therefore, the configuration $\bar{R}_0$ hits all $S \in \mathcal{S}$ since $\bar{R}_0$ is a transversal, so it is in *fail*($\mathcal{S}$). However this configuration is not in *fail*($\mathcal{R}$) since $\bar{R}_0$ does not hit R_0. Since $0 < p < 1$, both configurations R_0 and $\bar{R}_0$ have non-zero probability and the proposition follows. ∎

LEMMA 3.7. *If $\mathcal{S}$ is a dominated coterie then $F_p(\mathcal{S}) + F_{1-p}(\mathcal{S}) > 1$ for $0 < p < 1$.*

Proof. Let $\mathscr{R} \in \text{NDC}$ be such that $\mathscr{R} \succ \mathscr{S}$ (for any dominated coterie it is possible to find such an $\mathscr{R}$). Then using Lemma 3.6 and the symmetry Theorem 3.3 we get

$$F_p(\mathscr{S}) + F_{1-p}(\mathscr{S}) > F_p(\mathscr{R}) + F_{1-p}(\mathscr{R}) = 1. \quad \blacksquare$$

By plugging $p = 1/2$ and combining with Corollary 3.4 we get the two following results.

COROLLARY 3.8. *If $\mathscr{S}$ is a dominated coterie then* $F_{1/2}(\mathscr{S}) > 1/2$.

COROLLARY 3.9. $\mathscr{S} \in \text{NDC} \Leftrightarrow F_{1/2}(\mathscr{S}) = 1/2$.

The following proposition gives us a lower bound on the number of quorums in any $\mathscr{S} \in \text{NDC}$ in terms of the smallest quorum size $c = c(\mathscr{S})$. This extremal question has been addressed before in a slightly more general setting, i.e., lower bounds on the number of hyperedges of a non-2-colorable hypergraph (NDCs are 3-colorable hypergraphs [GB85]). Two results are presented in [AS92], a simple bound due to Erdős [Erd63] which gives $m \geqslant 2^{c-1}$, and a more delicate asymptotic bound due to Beck [Bec78] of $m \geqslant \Omega(2^c c^{1/3})$. We show, by a new proof, a bound that is better than the simple one yet is inferior to Beck's result.

PROPOSITION 3.10. *Let $\mathscr{S} \in \text{NDC}$ be given, let $m = m(\mathscr{S})$ be the number of quorums and let $c = c(\mathscr{S})$ be the cardinality of the smallest quorum. Then $m \geqslant 2^c \ln 2$.*

Proof. From the symmetry theorem we get

$$\tfrac{1}{2} = F_{1/2}(\mathscr{S}) = \mathbb{P}\left(\bigcap_{S \in \mathscr{S}} \mathscr{E}_S\right).$$

For any $S \in \mathscr{S}$ consider $\mathscr{E}_S$, the event that S is hit. Clearly $\mathscr{E}_S$ is a monotone increasing property (i.e., if a configuration X hits S then any configuration $X' \supseteq X$ hits S). Therefore we can use the FKG inequality [FKG71] to obtain

$$\mathbb{P}\left(\bigcap_{S \in \mathscr{S}} \mathscr{E}_S\right) \geqslant \prod_{S \in \mathscr{S}} \mathbb{P}(\mathscr{E}_S) = \prod_{S \in \mathscr{S}} \left(1 - \frac{1}{2^{|S|}}\right)$$
$$\geqslant \left(1 - \frac{1}{2^c}\right)^m \geqslant e^{-m/2^c},$$

and the proposition follows. $\blacksquare$

EXAMPLE Proposition 3.10 can be used to prove that a finite projective plane of order $t \geqslant 4$ is a dominated coterie (see also Section 5.6). This is because a finite projective plane of order t has $t^2 + t + 1$ quorums of cardinality $t + 1$, in violation of the necessary condition in Proposition 3.10 for $t \geqslant 4$.

4. MOST AND LEAST AVAILABLE NDCs

4.1. *Overview*

In this section, our main goal is to prove Theorem 4.5, stating that the ND coteries with the extreme failure probabilities are the singleton and the majority. More precisely, we show that when $0 < p < 1/2$, the worst ND coterie (i.e., for which F_p is highest) is the singleton, and the best ND coterie is the majority. When $1/2 < p < 1$ the situation is reversed (by the symmetry Theorem 3.3). The availability of these simple quorum systems, denoted by Sngl and Maj, is analyzed in Sections 5.1. and 5.5.

In Fig. 1 the functions $F_p(\text{Sngl})$ and $F_p(\text{Maj})$ are shown. By Theorem 4.5 and the symmetry theorem, for any $\mathscr{S} \in \text{NDC}$ the function $F_p(\mathscr{S})$ must be a symmetric function that lies inside the zones marked "ND" in the figure. The function $F_p(\mathscr{S})$ for dominated coteries might also lie in the zone marked "Dom."

Our proof generalizes the method of [BPT89]. Their work compares two specific quorum systems, namely the simple majority and a system called indirect majority, that models the election of the president of the United States. The proof has two conceptual stages. In Section 4.2, we prove some properties of the difference between the availability profiles of an arbitrary NDC and an extremal one (e.g., Sngl), by combinatorial considerations. Then in Section 4.3, these properties are transferred to the difference between the respective failure probabilities using the Variation Diminishing Property (VDP) of Totally Positive kernels [Kar68].

In Section 4.4, we show the uniqueness of the extremal NDCs. That is, we show that if $F_p(\mathscr{S}) = F_p(\text{Sngl})$ for any $\mathscr{S} \in \text{NDC}$ then $\mathscr{S}$ is a Sngl coterie. Also, over an odd sized universe, we show that if $F_p(\mathscr{S}) = F_p(\text{Maj})$ then $\mathscr{S}$ is Maj.

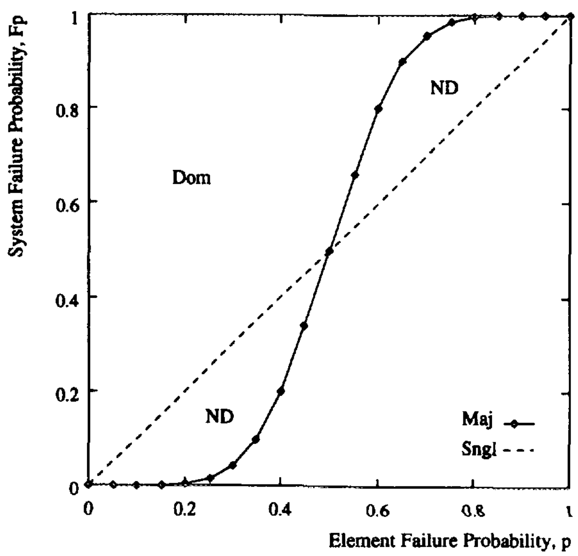

FIG. 1. The failure probabilities of the extremal coteries with $n = 17$.

Finally, in Section 4.5, we show that the "second worst" NDC is the Wheel coterie (see Section 5.1). Therefore, the Wheel is an extremal NDC when we require that each element $u \in U$ must participate in some quorum of the system, or alternatively, when it is forbidden that a single element participates in all the quorums.

4.2. *The Availability Profile of* Sngl *and* Maj

In this section, we present some properties of the availability profile of the extremal coteries, the singleton and majority coteries.

Fact 4.1. The availability profiles of the Sngl and Maj coteries are

- $a_i^{\mathrm{Sngl}} = \binom{n-1}{i-1}$ for $i = 0, ..., n$.
- $a_i^{\mathrm{Maj}} = \begin{cases} 0, & 0 \leqslant i < n/2, \\ \binom{n-1}{i-1}, & n \text{ even and } i = n/2, \\ \binom{n}{i}, & n/2 < i \leqslant n. \end{cases}$

The following lemma paves the way for proving the extremality of Sngl and Maj. Specifically, we prove that the availability profile of any $\mathscr{S} \in \mathrm{NDC}$ is "sandwiched" between the availability profiles of the Sngl and Maj coteries. It is this property that is the basis of Theorem 4.5.

LEMMA 4.2. *Let $\mathscr{S}$ be a given* ND *coterie over a universe U of size n. Then*

1. $a_i^{\mathrm{Maj}} \leqslant a_i^{\mathscr{S}} \leqslant a_i^{\mathrm{Sngl}}$ *for* $0 \leqslant i < n/2$,
2. $a_i^{\mathrm{Sngl}} \leqslant a_i^{\mathscr{S}} \leqslant a_i^{\mathrm{Maj}}$ *for* $n/2 < i \leqslant n$,
3. $a_i^{\mathrm{Sngl}} = a_i^{\mathscr{S}} = a_i^{\mathrm{Maj}} = \binom{n-1}{i-1}$ *when n is even and* $i = n/2$.

Proof. 1. Consider some $0 \leqslant i < n/2$. It is clear that $a_i^{\mathrm{Maj}} \leqslant a_i^{\mathscr{S}}$ since $a_i^{\mathrm{Maj}} = 0$ in this range of i. For the upper bound on $a_i^{\mathscr{S}}$, recall that $\mathscr{A}_i^{\mathscr{S}}$ is an intersecting hypergraph in $\mathscr{U}^{(i)}$ (Lemma 2.10). From the Sunflower Theorem 2.11, we conclude that $a_i^{\mathscr{S}} = |\mathscr{A}_i^{\mathscr{S}}| \leqslant \binom{n-1}{i-1} = a_i^{\mathrm{Sngl}}$.

2. Consider $n/2 < i \leqslant n$. Since $n - i < n/2$, case 1 yields $a_{n-i}^{\mathrm{Maj}} \leqslant a_{n-i}^{\mathscr{S}} \leqslant a_{n-i}^{\mathrm{Sngl}}$, hence

$$\binom{n}{i} - a_{n-i}^{\mathrm{Maj}} \geqslant \binom{n}{i} - a_{n-i}^{\mathscr{S}} \geqslant \binom{n}{i} - a_{n-i}^{\mathrm{Sngl}}.$$

Applying Lemma 3.1, the claim follows.

3. n is even and $i = n/2$: This is just a restatement of Corollary 3.2. ▮

4.3. *The Extremality Theorem*

With the groundwork prepared, we can now prove the extremality results.

DEFINITION 4.3. Let $\mathscr{S} \in \mathrm{NDC}$ be given. Then the *difference functions* of $\mathscr{S}$ w.r.t. Sngl and Maj are

- $f_{\mathscr{S}}^{\mathrm{Sngl}}(i) = a_i^{\mathrm{Sngl}} - a_i^{\mathscr{S}}$, for $i = 0, ..., n$.
- $f_{\mathrm{Maj}}^{\mathscr{S}}(i) = a_i^{\mathscr{S}} - a_i^{\mathrm{Maj}}$, for $i = 0, ..., n$.

The following claim, regarding the sign changes of $f_{\mathscr{S}}^{\mathrm{Sngl}}$ and $f_{\mathrm{Maj}}^{\mathscr{S}}$, is an immediate result of Lemma 4.2 (using Definition 2.13).

Claim 4.4. $S^-(f_{\mathscr{S}}^{\mathrm{Sngl}}) \leqslant 1$ and $S^-(f_{\mathrm{Maj}}^{\mathscr{S}}) \leqslant 1$. In both functions the sign change (if one occurs) is from + to − as i goes from 0 to n.

The following theorem establishes the extremal-availability quorum systems to be the singleton (Sngl) and majority (Maj). The left hand side inequality of claim 1 of the theorem is due to [BG87]. The left hand side inequality of claim 2 has been proved independently in [DKK+94]. The proof below proves all four inequalities at once.

THEOREM 4.5. *Let $\mathscr{S} \in \mathrm{NDC}$ be given. Then*

1. $p < 1/2 \Rightarrow F_p(\mathrm{Maj}) \leqslant F_p(\mathscr{S}) \leqslant F_p(\mathrm{Sngl})$.
2. $p > 1/2 \Rightarrow F_p(\mathrm{Sngl}) \leqslant F_p(\mathscr{S}) \leqslant F_p(\mathrm{Maj})$.

Proof. We start by proving the relations between $F_p(\mathscr{S})$ and $F_p(\mathrm{Sngl})$. Using the definitions of F_p and $f_{\mathscr{S}}^{\mathrm{Sngl}}$, define

$$\begin{aligned} g^{\mathrm{Sngl}}(p) &= F_p(\mathrm{Sngl}) - F_p(\mathscr{S}) \\ &= \sum_{i=0}^{n} (a_i^{\mathrm{Sngl}} - a_i^{\mathscr{S}})\, p^i (1-p)^{n-i} \\ &= \sum_{i=0}^{n} f_{\mathscr{S}}^{\mathrm{Sngl}}(i)\, p^i (1-p)^{n-i}. \end{aligned}$$

We need to show that $g^{\mathrm{Sngl}}(p)$ is nonnegative when $p \leqslant 1/2$ and nonpositive when $p \geqslant 1/2$. If $g^{\mathrm{Sngl}} \equiv 0$ we are done, therefore assume otherwise. As stated in Fact 2.15, the kernel $K(p, i) = p^i(1-p)^{n-i}$ is totally positive. Therefore we can use the VDP Theorem 2.14 to get

$$S^-(g^{\mathrm{Sngl}}) \leqslant S^-(f_{\mathscr{S}}^{\mathrm{Sngl}}).$$

Applying Claim 4.4, we get that $S^-(g^{\mathrm{Sngl}}) \leqslant 1$.

We know from Fact 2.19 and Corollary 3.4 that for any $\mathscr{S} \in \mathrm{NDC}$, $g^{\mathrm{Sngl}}(0) = g^{\mathrm{Sngl}}(1/2) = g^{\mathrm{Sngl}}(1) = 0$. Now $g^{\mathrm{Sngl}}(p)$ is not identically zero. By the symmetry Theorem 3.3 it follows that $g^{\mathrm{Sngl}}(p) > 0$ iff $g^{\mathrm{Sngl}}(1-p) < 0$, so it has strictly positive and negative points. Therefore $S^-(g^{\mathrm{Sngl}}) > 0$, so $S^-(g^{\mathrm{Sngl}}) = 1$, and since g^{Sngl} is a polynomial the sign change is at 1/2.

Again by the VDP theorem, g^{Sngl} has the same sequence of signs as $f_{\mathscr{S}}^{\mathrm{Sngl}}$, namely, g^{Sngl} goes from + to − as p goes from 0 to 1. We conclude that $F_p(\mathscr{S}) \leqslant F_p(\text{Sngl})$ when $p < 1/2$, and $F_p(\text{Sngl}) \leqslant F_p(\mathscr{S})$ when $p > 1/2$.

Repeating the same argument using $f^{\mathscr{S}}_{\text{Maj}}$ completes the proof. ∎

Remark. An alternative proof for Theorem 4.5 has been suggested to us [Hol93]. The proof uses the notion of *majorization* [MO79] and the fact that $k_i = p^i(1-p)^{n-i}$ is a decreasing sequence for $i = 0, ..., n$ when $p < 1/2$.

4.4. *Uniqueness of the Extremal* NDCs

In this section, we show the uniqueness of the failure probability of the Sngl coterie, and of the Maj coterie over an odd sized universe (Proposition 4.11).

The proof of the non-trivial part of these claims is presented in two steps. First we prove that if $\mathscr{S}$ is not a Sngl coterie then its availability profile is not a^{Sngl}, and that if n is odd and $\mathscr{S}$ is not Maj then $a^{\mathscr{S}} \neq a^{\text{Maj}}$. Then we prove that if $a^{\mathscr{S}} \neq a^{\text{Sngl}}$ then $F_p(\mathscr{S}) \neq F_p(\text{Sngl})$, and similarly for Maj.

Unless otherwise stated, we assume that all the coteries are ND, over a universe U of size n.

LEMMA 4.6. *If* $a_i^{\mathscr{S}} = a_i^{\text{Sngl}} = \binom{n-1}{i-1}$ *for* $0 \leqslant i \leqslant n$ *then* $\mathscr{S} = \{\{u\}\}$ *for some* $u \in U$.

Proof. Specifically, $a_1^{\mathscr{S}} = 1$. Therefore there exists $u \in U$ such that the set $\{u\}$ hits all $S \in \mathscr{S}$. Hence $u \in S$ for all $S \in \mathscr{S}$. If $\mathscr{S} \neq \{\{u\}\}$ then $\{\{u\}\}$ dominates $\mathscr{S}$, contradiction to the premise that $S \in \text{NDC}$. ∎

For the proof of uniqueness of the availability profile of the Maj coterie we need the following lemma, which shows that the number of minimal cardinality quorums is easily seen in the availability profile.

LEMMA 4.7. *Let* $\mathscr{S} \in \text{NDC}$, *and* $r = \min\{i : a_i^{\mathscr{S}} > 0\}$. *Then*

(a) *All the transversals of size r are quorums, i.e.,* $\mathscr{A}_r^{\mathscr{S}} = \{S \in \mathscr{S} : |S| = r\}$.

(b) *The minimal quorum size* $c(\mathscr{S}) = r$.

Proof. Consider some transversal $X \in \mathscr{A}_r^{\mathscr{S}}$. By Lemma 2.7 there exists a quorum $S \in \mathscr{S}$ such that $S \subseteq X$. Obviously $|X| = r$ implies $|S| \leqslant r$, hence $c(\mathscr{S}) \leqslant r$. It is impossible that $c(\mathscr{S}) < r$ since every $S \in \mathscr{S}$ is a transversal, and the minimal transversal size is r, thus proving (b). Additionally, $S = X$, proving (a). ∎

LEMMA 4.8. *Suppose* $n = 2t + 1$, *and*

$$a_i^{\mathscr{S}} = \begin{cases} 0, & 0 \leqslant i \leqslant t, \\ \binom{n}{i}, & t+1 \leqslant i \leqslant n. \end{cases}$$

Then $\mathscr{S}$ *is* Maj.

Proof. By Lemma 4.7(b), $c(\mathscr{S}) = t + 1$. Moreover, $a_{t+1}^{\mathscr{S}} = \binom{n}{t+1}$ so every set of size $t+1$ is a transversal. By Lemma 4.7(a), every set of size $t + 1$ is in $\mathscr{S}$. From the Minimality property of NDCs, no sets of size greater than $t + 1$ can belong to $\mathscr{S}$. Hence $\mathscr{S} = \text{Maj}$. ∎

Remark. If n is even then there exist several NDC constructions with an availability profile identical to a^{Maj} (as described in Fact 4.1). To see this, assume that $n = 2t$. One possible construction is the one we have used before; discard an element u from U and use the (unique) Maj over an odd sized universe. Another possibility is best defined by voting; pick an element u, assign a vote of 2 to it, and assign a vote of 1 to all the other elements. The latter construction has quorums of size t (that contain u) and of size $t + 1$ (without u). It is easy to verify that both constructions have an availability profile identical to a^{Maj}.

To show the uniqueness of the failure probabilities, we need the following lemma, which describes a general property of the difference between two availability profiles.

LEMMA 4.9. *Let* $\mathscr{S}, \mathscr{R} \in \text{NDC}$ *be given over the same universe U. Let* $f^{\mathscr{S}}_{\mathscr{R}}(i) = a_i^{\mathscr{S}} - a_i^{\mathscr{R}}$ *for* $i = 0, ..., n$. *Then* $f^{\mathscr{S}}_{\mathscr{R}}(i) = -f^{\mathscr{S}}_{\mathscr{R}}(n-i)$ *for* $i = 0, ..., n$.

Proof. Using Lemma 3.1 we get

$$f^{\mathscr{S}}_{\mathscr{R}}(i) = \binom{n}{i} - a^{\mathscr{S}}_{n-i} - \binom{n}{i} + a^{\mathscr{R}}_{n-i} = -f^{\mathscr{S}}_{\mathscr{R}}(n-i). \quad ∎$$

LEMMA 4.10. *If* $a^{\mathscr{S}} \neq a^{\text{Sngl}}$ *then* $F_p(\mathscr{S}) \neq F_p(\text{Sngl})$, *and if* $a^{\mathscr{S}} \neq a^{\text{Maj}}$ *then* $F_p(\mathscr{S}) \neq F_p(\text{Maj})$.

Proof. Consider the difference function $f^{\text{Sngl}}_{\mathscr{S}}$ (as in Definition 4.3). By Lemma 4.9, $f^{\text{Sngl}}_{\mathscr{S}}(i) = -f^{\text{Sngl}}_{\mathscr{S}}(n-i)$ for all i. Fix some arbitrary $0 < p < 1/2$. Then

$$\begin{aligned} F_p(\text{Sngl}) - F_p(\mathscr{S}) &= \sum_{i=0}^{n} f^{\text{Sngl}}_{\mathscr{S}}(i)\, p^i q^{n-i} \\ &= \sum_{0 \leqslant i < n/2} f^{\text{Sngl}}_{\mathscr{S}}(i)(p^i q^{n-i} - p^{n-i} q^i) \\ &= \sum_{0 \leqslant i < n/2} f^{\text{Sngl}}_{\mathscr{S}}(i)\, p^i q^i (q^{n-2i} - p^{n-2i}). \end{aligned}$$

Since $p < 1/2 < q$, and since by Lemma 4.2 $f^{\text{Sngl}}_{\mathscr{S}}(i) \geqslant 0$ when $i < n/2$, all the terms in the last sum are non-negative. By the premise $a^{\mathscr{S}} \neq a^{\text{Sngl}}$, therefore there exists an i for which $a_i^{\mathscr{S}} \neq a_i^{\text{Sngl}}$, hence $f^{\text{Sngl}}_{\mathscr{S}}(i) \neq 0$. By Lemma 4.9, we can assume w.l.o.g. that $i < n/2$, so $f^{\text{Sngl}}_{\mathscr{S}}(i) > 0$. This implies that the above sum is strictly positive, hence $F_p(\text{Sngl}) \neq F_p(\mathscr{S})$.

For the Maj, we start with $F_p(\mathscr{S}) - F_p(\text{Maj})$ and follow the same argument. ∎

Proposition 4.11 (Uniqueness). *Let $\mathcal{S} \in$ NDC. Then $F_p(\mathcal{S}) = F_p(\text{Sngl})$ iff $\mathcal{S}$ is a* Sngl *coterie. If $n = |U|$ is odd then $F_p(\mathcal{S}) = F_p(\text{Maj})$ iff $\mathcal{S}$ is the* Maj *coterie.*

Proof. If $\mathcal{S}$ is a Sngl or Maj coterie the claim is trivial. If $\mathcal{S}$ is not a Sngl coterie, then by Lemma 4.6, $a^{\mathcal{S}} \neq a^{\text{Sngl}}$. If n is odd and $\mathcal{S}$ is not a Maj coterie, then by Lemma 4.8, $a^{\mathcal{S}} \neq a^{\text{Maj}}$. Therefore by Lemma 4.10 the result follows. ∎

4.5. *The Worst* NDC *Using the Entire Universe*

In Theorem 4.5, we saw that the Sngl is the NDC with the worst availability (when $0 < p < 1/2$). However, the Sngl coterie does not "scale up" in the true sense of the word when the universe size n increases, since all but one of the elements of U do not appear in any quorum. It is sometimes required, for load distribution purposes, that every element $u \in U$ must participate in some $S \in \mathcal{S}$. Call such coteries *total* coteries. We can ask which total ND coterie has the worst availability.

In this section, we show that the Wheel NDC is the wanted extremal coterie (Proposition 4.14).

Remark. It is interesting to note that the requirement of using all the elements does not significantly improve the situation in terms of the worst possible availability. In particular, $F_p(\text{Wheel}) \to_{n\to\infty} p = F_p(\text{Sngl})$, for any $0 < p < 1$.

Fact 4.12. The availability profile of the *Wheel* coterie is

$$a_i^{\text{Wheel}} = \begin{cases} 0, & 0 \leqslant i \leqslant 1, \\ \binom{n-1}{i-1}, & 2 \leqslant i \leqslant n-2, \\ \binom{n}{i}, & n-1 \leqslant i \leqslant n. \end{cases}$$

For the proof of Proposition 4.14, we need the following lemma. The lemma implies that for any $\mathcal{S} \in$ NDC, if $a_i^{\mathcal{S}} = \binom{n-1}{i-1}$ for some $i < n/2$ then $a_j^{\mathcal{S}} = \binom{n-1}{j-1}$ for all $i \leqslant j < n/2$.

Lemma 4.13. *Let $\mathcal{S} \in$ NDC, and suppose there is an index i, $1 \leqslant i < (n/2) - 1$, with $a_i^{\mathcal{S}} = \binom{n-1}{i-1}$. Then $a_{i+1}^{\mathcal{S}} = \binom{n-1}{i}$.*

Proof. Assume that $a_i^{\mathcal{S}} = \binom{n-1}{i-1}$ for some $1 \leqslant i < (n/2) - 1$. Then by the Sunflower Theorem 2.11, $\mathcal{A}_i^{\mathcal{S}}$ is a "sunflower," i.e., there exists an element u_0 such that $u_0 \in X$ for all $X \in \mathcal{A}_i^{\mathcal{S}}$. Now consider $\mathcal{A}_{i+1}^{\mathcal{S}}$. $\mathcal{A}_{i+1}^{\mathcal{S}}$ is an intersecting hypergraph in $U^{(i+1)}$, so again by the Sunflower Theorem,

$$a_{i+1}^{\mathcal{S}} \leqslant \binom{n-1}{i}. \qquad (*)$$

In the other direction, for any $X \in \mathcal{A}_i^{\mathcal{S}}$ and $Y \supset X$ such that $Y \in U^{(i+1)}$, it is obvious that Y hits all $S \in \mathcal{S}$, so $Y \in \mathcal{A}_{i+1}^{\mathcal{S}}$. Therefore

$$a_{i+1}^{\mathcal{S}} \geqslant |\{X \cup \{w\} : X \in \mathcal{A}_i^{\mathcal{S}}, w \in U \backslash X\}|.$$

But the last expression is precisely the number of sets of size $i+1$ that contain u_0, i.e.,

$$a_{i+1}^{\mathcal{S}} \geqslant \binom{n-1}{i}. \qquad (**)$$

Combining $(*)$ and $(**)$, the lemma follows. ∎

Proposition 4.14. *Let $\mathcal{S} \in$ NDC be such that every element $u \in U$ is in some $S \in \mathcal{S}$. Then for $0 < p < 1/2$, $F_p(\mathcal{S}) \leqslant F_p(\text{Wheel})$.*

Proof. Fix $0 < p < 1/2$, and consider the coterie $\mathcal{S} \in$ NDC with the maximal $F_p(\mathcal{S})$ which uses all the elements of U. For this $\mathcal{S}$, define the difference function w.r.t. the Sngl coterie, $f_{\mathcal{S}}^{\text{Sngl}}(i) = a_i^{\text{Sngl}} - a_i^{\mathcal{S}}$. As in the proof of Lemma 4.10, and using $F_p(\text{Sngl}) = p$, we get

$$F_p(\mathcal{S}) = p - \sum_{0 \leqslant i < n/2} f_{\mathcal{S}}^{\text{Sngl}}(i)\, p^i q^i (q^{n-2i} - p^{n-2i}).$$

We need to estimate how large $F_p(\mathcal{S})$ might be. When $i < n/2$ and $p < 1/2 < q$ the parenthesized expressions are positive. Additionally, by Lemma 4.2, $f_{\mathcal{S}}^{\text{Sngl}}(i) \geqslant 0$ when $0 \leqslant i < n/2$. Thus, $F_p(\mathcal{S})$ is "large" whenever $f_{\mathcal{S}}^{\text{Sngl}}(i) = 0$ for "many" values of i, $i < n/2$.

It is not the case that $f_{\mathcal{S}}^{\text{Sngl}}(i) > 0$ for all $0 \leqslant i < n/2$. This is because for the Wheel coterie $f_{\mathcal{S}}^{\text{Sngl}}(2) = 0$, hence for $\mathcal{S}$ with the maximal $F_p(\mathcal{S})$ there is some $i < n/2$ such that $f_{\mathcal{S}}^{\text{Sngl}}(i) = 0$ and $0 \leqslant i < n/2$. Let $t[\mathcal{S}] = \min\{i : f_{\mathcal{S}}^{\text{Sngl}}(i) = 0\}$. By Lemma 4.13, $f_{\mathcal{S}}^{\text{Sngl}}(i) = 0$ for all $t[\mathcal{S}] \leqslant i < n/2$. Therefore the maximal value for $F_p(\mathcal{S})$ is when $t[\mathcal{S}]$ is the smallest possible. $t[\mathcal{S}]$ cannot be 1 since by the uniqueness of Sngl (Proposition 4.11), $t[\mathcal{S}] = 1$ would imply that $\mathcal{S}$ is a Sngl coterie, which does not use all the elements of the universe. We conclude that for the NDC with the worst availability that uses all the elements, $t[\mathcal{S}] = 2$, i.e., $f_{\mathcal{S}}^{\text{Sngl}}(1) = 1$ and $f_{\mathcal{S}}^{\text{Sngl}}(i) = 0$ for all $2 \leqslant i < n/2$. But this implies that $a^{\mathcal{S}} = a^{\text{Wheel}}$, and $F_p(\mathcal{S}) = F_p(\text{Wheel})$. ∎

5. THE AVAILABILITY OF COTERIE CONSTRUCTIONS

In this section, we analyze several coterie constructions that have appeared in the literature. Before showing the details of the constructions, we first present their properties concisely in Table 1. For each coterie construction we list the number of quorums $m(\mathcal{S})$, the minimal quorum cardinality $c(\mathcal{S})$, the failure probability $F_p(\mathcal{S})$, and whether $F_p(\mathcal{S})$ is Condorcet. Recall that by Definition 2.22, $F_p(\mathcal{S})$ is Condorcet iff $F_p(\mathcal{S}) \to_{n\to\infty} 0$ when $p < 1/2$ and $F_p(\mathcal{S}) \to_{n\to\infty} 1$ when $p > 1/2$.

TABLE 1

Properties of Coterie Constructions

$\mathcal{S}$	$m(\mathcal{S})$	$c(\mathcal{S})$	$F_p(\mathcal{S})$	Condorcet
Sngl	1	1	p	No
Wheel	n	2	$p-pq(q^{n-2}-p^{n-2})$	No
Triang	$\approx(e-1)(\sqrt{2n})!$	$\approx\sqrt{2n}$	$\geqslant p^{1/p}$	No
Tree	$2^{(n+1)/2}-1$	$\log_2(n+1)$	$\leqslant n^{-\varepsilon(p)}$	Yes
Nuc	$\approx 4n$	$\approx\frac{1}{2}\log_2 n$	$\leqslant n^{-\varepsilon(p)}$	Yes
Maj	$\binom{n}{(n+1)/2}>2^{n-1}/\sqrt{n}$	$(n+1)/2$	$\leqslant e^{-\varepsilon(p)n}$	Yes
FPP	n	$\approx\sqrt{n}$	$\geqslant(1-q^{\sqrt{n}})^n$	No
Grid	$\sqrt{n}^{\sqrt{n}}$	$2\sqrt{n}-1$	$\geqslant(1-q^{\sqrt{n}})^{\sqrt{n}}$	No

Remarks.

- All the coteries are over a universe of size n.
- Most constructions require special universe sizes (e.g., $n=2^t-1$ for some t); these details are omitted from the table.
- We use $\varepsilon(p)$ to denote expressions depending solely on p. The precise value in each case depends on the construction.
- The failure probability F_p is presented for the case of $0<p<1/2$. This characterizes F_p completely for NDC systems, since by the symmetry Theorem 3.3 $F_p(\mathcal{S})=1-F_{1-p}(\mathcal{S})$ for any $\mathcal{S}\in$ NDC.
- Instead of exact expressions, we present bounds on F_p that emphasize its asymptotic behavior and explain why each construction is or is not Condorcet.
- The first six rows in the table represent non-dominated coteries and the last two rows represent dominated ones. Note that in both the latter cases, $F_p(\mathcal{S})\to_{n\to\infty} 1$ for *any* value $0<p<1$, so these constructions have poor availability for all but very small systems.

5.1. *The* Sngl *and* Wheel *Coteries*

The Sngl system is the trivial singleton NDC, $\mathcal{S}=\{\{a\}\}$. This coterie corresponds to the centralized mutual exclusion protocol where a single processor controls the access to the critical section. It is also called the "monarchy" for obvious reasons.

The Wheel coterie is an "almost centralized" system. To calculate $F_p(\text{Wheel})$ observe that in a failure configuration, either the hub and at least one other element fail, or the hub does not fail and all others do, therefore we have

$$F_p(\text{Wheel})=p(1-q^{n-1})+qp^{n-1}=p-pq(q^{n-2}-p^{n-2}).$$

5.2. *The* Triang *Coterie*

The Triang system was first described in [Lov73, EL75] and proved to be ND in [Nei92, MP92a]. The elements are organized in a triangular grid of d rows, with the ith row containing i elements (we assume $n=d(d+1)/2$). A quorum is made of the elements of one complete row i, and a representative from each row $j>i$ (see Fig. 2). It is obvious that $c(\text{Triang})=d$, and not hard to see that $m(\text{Triang})=\lfloor(e-1)\,d!\rfloor$ (cf. [Lov73]).

To compute $F_p(\text{Triang})$, consider the following procedure to search the triangle for either a complete quorum or a failure configuration. We go over the rows from the bottom up, starting with row d. At row i we have three options:

1. If all i elements in the row have failed, stop; the system has failed.
2. If all i elements in the row have succeeded, stop; there is a complete functioning quorum in the system.
3. Otherwise, continue to row $i-1$.

A moment's reflection reveals that the procedure considers row $i-1$ only if row i has both a failed element and a successful one, thus both stopping decisions are correct. There is no special rule for row 1; since it contains a single element is must fall into one of the stopping cases.

Let $F_p(d)$ denote F_p of a Triang of d rows. Then the above procedure gives the recurrence

$$F_p(d)=p^d+(1-p^d-q^d)\,F_p(d-1),$$

and after expansion we get

$$F_p(d)=\sum_{i=1}^{d} p^i\left(\prod_{j=i+1}^{d}(1-p^j-q^j)\right).$$

In order to show that $F_p(\text{Triang})$ is *not* Condorcet, we bound it from below. The system certainly fails if there is no row in which all the elements succeed, i.e.,

$$F_p(d)\geqslant\mathbb{P}(\text{no row is completely successful})=\prod_{i=1}^{d}(1-q^i).$$

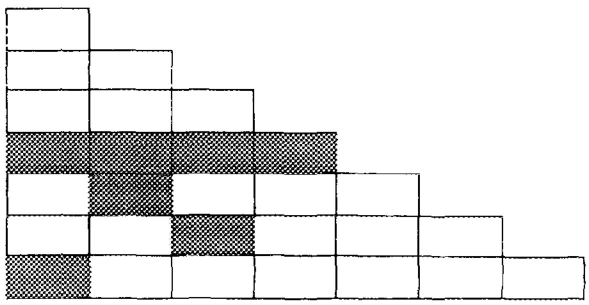

FIG. 2. A 28-element Triang coterie, with one quorum shaded.

Consider the function $h(x)=e^{-kx}$ for $k>1$. This function crosses the function $1-x$ twice, at $x=0$ and at $x=t$ for some $0<t<1$ that satisfies

$$k=\frac{1}{t}\ln\frac{1}{1-t}.$$

Moreover, $1-x\geqslant h(x)$ in the range $0\leqslant x\leqslant t$. Thus for the success probability q, if

$$k=\frac{1}{q}\ln\frac{1}{p}$$

then $1-q^i\geqslant e^{-kq^i}$ for all $i\geqslant 1$ since $0<q^i<q$. Therefore

$$\prod_{i=1}^{d}(1-q^i)\geqslant e^{-k\sum_{i=1}^{d}q^i}\geqslant e^{-k(q/p)}.$$

Plugging in the value of k we conclude that $F_p(\text{Triang})\geqslant p^{1/p}$, for any number of rows, thus $F_p(\text{Triang})$ is not Condorcet.

5.3. *The Tree Coterie*

The Tree system was first described and proved to be a coterie in [AE91]. In [IK93, NM92], it is shown that Tree ∈ NDC. The elements are organized in a complete rooted binary tree (we assume that $n=2^h-1$ for some $h>0$). For a node v let $T(v)$ denote the tree rooted at v, and let $T_L(v)$ and $T_R(v)$ denote the left and right subtrees of v respectively. Then a quorum in the system is defined recursively by the following procedure $QE(T(v))$ (Quorum Extract).

1. For a leaf v, $QE(T(v))$ is taken to be $\{v\}$.
2. Either take the root, and a quorum in the subtree of one of the root's children.
3. Or take the union of two quorums, one from the subtree of each child.

Formally,

$$QE(T(v))\leftarrow\begin{cases}\{v\}, & v \text{ is a leaf},\\ \{v\}\cup QE(T_L(v)) \quad \text{OR} & \\ \{v\}\cup QE(T_R(v)) \quad \text{OR} & \\ QE(T_L(v))\cup QE(T_R(v)), & \text{otherwise.}\end{cases}$$

To calculate $m(\text{Tree})$, define $m(h)$ to be the number of quorums in a Tree system of height h. Then $m(h)$ obeys the recurrence

$$m(h)=2m(h-1)+(m(h-1))^2,$$

and $m(1)=1$. The solution is $m(h)=2^{2^{h-1}}-1$, and plugging $2^h=n+1$ we get that $m(\text{Tree})=2^{(n+1)/2}-1$. It is clear that $c(\text{Tree})=\log_2(n+1)$.

For the calculation of $F_p(\text{Tree})$, define $F_p(h)$ to be F_p of a Tree with height h. Then $F_p(1)=p$, and

$$\begin{aligned}F_p(h)&=p\cdot\mathbb{P}(\text{at least one subtree fails})\\&\quad+(1-p)\cdot\mathbb{P}(\text{both subtrees fail})\\&=p(1-(1-F_p(h-1))^2)+(1-p)(F_p(h-1))^2\\&=2pF_p(h-1)+(1-2p)(F_p(h-1))^2.\end{aligned}$$

A simple check shows that if $p=1/2$ then $F_p(h)=1/2$ for all h. Using the sufficient condition of Proposition 3.9, we obtain that Tree ∈ NDC, without the case analysis required in a direct proof.

It is easy to prove by induction that if $p<1/2$ then $F_p(h)\leqslant p$ and then that $F_p(h)\leqslant(p+1/2)^h$. Plugging $h=\log_2(n+1)$ we get that $F_p(\text{Tree})\leqslant n^{-\varepsilon(p)}$ for some constant $\varepsilon(p)>0$ depending on p. Therefore, using the symmetry Theorem 3.3, we conclude that $F_p(\text{Tree})$ is Condorcet.

5.4. *The* Nuc *Coterie*

The *nucleus* (Nuc) system appears first in [EL75], and a variation appears in [Tuz85]. The system is built in two stages. First consider a nucleus universe U_1 of size $2r-2$ for some $r>1$, and add to $\mathcal{S}$ all the subsets of U_1 of size r. Secondly, for each possible partition of U_1 into two disjoint sets T'_j, T''_j with $|T'_j|=|T''_j|=r-1$, add a new element x_j to the universe and add the sets $T'_j\cup\{x_j\}$ and $T''_j\cup\{x_j\}$ to $\mathcal{S}$. It is easy to check directly that Nuc ∈ NDC.

After both steps, the universe size is

$$n=2r-2+\frac{1}{2}\binom{2r-2}{r-1}.$$

Therefore $c(\text{Nuc})\approx(1/2)\log_2 n$. The number of quorums is

$$m(\text{Nuc})=\binom{2r-2}{r}+\binom{2r-2}{r-1}=\frac{1}{2}\binom{2r}{r}\approx 4n.$$

The Nuc system has some interesting extremal properties [EL75]. In particular, it serves as an extreme case for a coterie for which it is hard to balance the load among the processors [HMP95].

In order to compute $F_p(\text{Nuc})$, note that any transversal T of the system has $|T\cap U_1|\geqslant r-1$, since Nuc ∈ NDC. Therefore

$$F_p(\text{Nuc})\leqslant\mathbb{P}(\text{at least } r-1 \text{ failures in } U_1).$$

The expected number of failures in U_1 is $(2r-2)p$. If $p<1/2$ we can write $r-1=(1+\delta)(2r-2)p$ and use the standard Chernoff bound [Che52] to get

$$F_p(\text{Nuc}) \leqslant e^{-(2r-2)p\delta^2/3} \leqslant n^{-\varepsilon(p)}$$

for some constant $\varepsilon(p)>0$, so $F_p(\text{Nuc})$ is Condorcet.

5.5. *The* Maj *Coterie*

The Condorcet Jury Theorem [Con] is in fact about the asymptotic behavior of the Maj coterie, so naturally $F_p(\text{Maj})$ is Condorcet. To estimate the rate of convergence, if $p<1/2$, the failure probability is

$$F_p(\text{Maj}) \leqslant \mathbb{P}(\text{at least } (n+1)/2 \text{ failures}) \leqslant e^{-\varepsilon(p)n}$$

for some constant $\varepsilon(p)>0$, using the Chernoff bound.

5.6. *The* FPP *Coterie*

The FPP coterie is based on finite projective planes, and appears first in a mutual exclusion protocol in [Mae85]. For a prime r let $t=r^k$ for some integer k. Then the finite projective plane of order t is a quorum system with $m(\text{FPP})=t^2+t+1$ quorums, each of size $c(\text{FPP})=t+1$. It has been shown in [Fu90] that for all $t\geqslant 3$, the FPP of order t is dominated. The only non-dominated FPP is of order 2, i.e., the 7 point Fano plane. The asymptotic behavior of the FPPs availability has been shown in [RST92], and we include it for completeness.

Let $F_p(t)$ denote $F_p(\text{FPP})$ for a finite projective plane of order t. To bound $F_p(t)$ from below, we apply the same argument as in the proof of Proposition 3.10 and use the FKG inequality. We get

$$F_p(t) \geqslant \prod_{S\in \text{FPP}} (1-q^{|S|}) = (1-q^{t+1})^{t^2+t+1} \xrightarrow[t\to\infty]{} 1.$$

Note that this holds for *any* $p>0$. Therefore, the FPP coterie has poor availability in all but very small systems.

5.7. *The* Grid *Coterie*

The Grid coterie appears in [CAA90, MP92a]. The $n=d^2$ elements are arranged in a $d\times d$ grid, and a quorum in the system consists of one complete row and a representative element from all the other rows. There are $m(\text{Grid})=d^d$ quorums, all of size $c(\text{Grid})=2d-1$. To see that Grid is dominated, consider the set of elements on the diagonal—it is a transversal of the system but is not a superset of any quorum.

Let $F_p(d)$ denote $F_p(\text{Grid})$ for a $d\times d$ grid. To bound $F_p(d)$ from below, note that for the system to fail it is enough to have at least one failure per row. Therefore, as shown in [KC91],

$$F_p(d) \geqslant \mathbb{P}(\text{at least one failure per row}) = (1-q^d)^d \xrightarrow[d\to\infty]{} 1.$$

6. THE AVAILABILITY OF WEIGHTED VOTING

A simple and popular method to define and implement quorum systems is by weighted voting [Gif79, GB85, BG86, AAC91, MP92a]. In a voting system, each element is assigned a number of votes, and a quorum is any subset of elements with a weight exceeding half of the total weight. In this section we consider voting systems over a universe of size n for increasing n. We give two necessary conditions that ensure that the failure probability of such systems is Condorcet.

DEFINITION 6.1. For each $i\in U$ let the integer $w_i\geqslant 0$ denote the *weight* of i. Let $W=\sum_i w_i$ be the *total weight*. The *full voting system* defined by the weights w_i is

$$\text{Vote}_\text{F} = \left\{ S\subseteq U : \sum_{i\in S} w_i > \frac{W}{2} \right\}.$$

As defined above, Vote_F is not a coterie since it does not satisfy the Minimality property. To amend this situation, we discard all the quorums that are supersets of other quorums.

DEFINITION 6.2. Let the *Voting Coterie* defined by the weights w_i be

$$\text{Vote} = \{ S\in \text{Vote}_\text{F} : \forall u\in S,\ S\backslash\{u\} \notin \text{Vote}_\text{F} \}.$$

In [GB85], it is shown that if the total weight W is odd then $\text{Vote}\in\text{NDC}$. If W is even then either Vote is dominated, or there exists a different distribution of weights w' with an odd total that defines the same (non-dominated) Vote coterie. Therefore for simplicity we shall assume that W is odd. In this case, we can define Vote_F (and its coterie Vote) by taking as a quorum any set $S\subseteq U$ such that $\sum_{i\in S} w_i \geqslant W/2$.

PROPOSITION 6.3. *Let* Vote *be defined by weights* w_i *with an odd total* W. *Let the maximal weight be* $w_{\max}=\max_i\{w_i\}$. *Then*

- $0<p<1/4e \Rightarrow F_p(\text{Vote}) < 2^{-W/2w_{\max}}$,
- $1/4e \leqslant p < 1/2 \Rightarrow F_p(\text{Vote}) < e^{-((1-2p)^2/16p)\cdot(W/w_{\max})}$.

Therefore $F_p(\text{Vote})$ *is Condorcet if* $W/w_{\max} \to_{n\to\infty} \infty$.

Proof. Define a Bernoulli random variable X_i for each element $i\in U$, $X_i=1$ when the element i fails. Then $X_i\sim B(p)$. Let the total weight of the failed elements be $Z=\sum_{i=1}^n w_iX_i$. The system fails exactly when $Z\geqslant W/2$. We want to bound the probability of this event using the Chernoff-type bound for weighted sums, due to Raghavan and Spencer [Rag88]. For this bound to be applicable, the weights need to be at most 1. Therefore we scale the weights by a factor of $w_{\max}$, defining

$$\hat{w}_i = \frac{w_i}{w_{\max}}, \qquad i = 1, \ldots, n.$$

Clearly $0 < \hat{w}_i \leqslant 1$. Let $\hat{Z} = \sum_{i=1}^{n} \hat{w}_i X_i = Z/w_{\max}$ and $\hat{W} = W/w_{\max}$. Then

$$F_p(\text{Vote}) = \mathbb{P}\left(\hat{Z} \geqslant \frac{\hat{W}}{2}\right).$$

The expectation of $\hat{Z}$ is

$$\mathbb{E}[\hat{Z}] = \sum_{i=1}^{n} \hat{w}_i \cdot p = p \cdot \hat{W}.$$

Set $\delta = (1-2p)/2p$. If $p < 1/2$ then $\delta > 0$ so we can write $\hat{W}/2 = (1+\delta)\, \mathbb{E}[\hat{Z}]$. By the Raghavan–Spencer bound,

$$\mathbb{P}\left(\hat{Z} \geqslant \frac{\hat{W}}{2}\right) < \left[\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right]^{\mathbb{E}[\hat{Z}]}.$$

Using standard estimations of the last expression when $\delta > 2e-1$ and when $\delta \leqslant 2e-1$ completes the proof. ∎

We now give a different bound of $F_p(\text{Vote})$, based on the Chebicheff inequality.

PROPOSITION 6.4. *Let* Vote *be defined by weights w_i with an odd total W. If $p < 1/2$ then*

$$F_p(\text{Vote}) \leqslant \frac{pq}{(1/2-p)^2} \cdot \frac{\sum_i w_i^2}{W^2}.$$

Therefore $F_p(\text{Vote})$ is Condorcet if $\sum_i w_i^2/W^2 \to_{n\to\infty} 0$.

Proof. Define X_i and Z as in the proof of Proposition 6.3. To use the Chebicheff bound we need the expectation and variance of Z.

$$\mathbb{E}[Z] = Wp,$$
$$V(Z) = \sum_i w_i^2 pq.$$

Clearly Z is a positive r.v., and when $p < 1/2$ then $W/2 - \mathbb{E}[Z] > 0$ so we can apply the Chebicheff bound to get

$$F_p(\text{Vote}) = \mathbb{P}\left(Z \geqslant \frac{W}{2}\right) \leqslant \frac{pq \sum_i w_i^2}{(W/2 - Wp)^2},$$

and the claim follows. ∎

Remark. At first glance Proposition 6.4 seems to be much weaker than the exponential decay shown in Proposition 6.3. However there are cases when the seemingly weaker bound is more useful. Consider the voting system defined as follows. There are $n = 2d+1$ elements for some odd d, a single element with weight d, and all the others with weight 1. Then $W = 3d$, and the ratios are $W/w_{\max} = 3$ and $\sum_i w_i^2/W^2 \approx 1/9$. The system does not satisfy either of the conditions for being Condorcet (and in fact $F_p(\text{Vote})$ is *not* Condorcet in this case). But when we check the values guaranteed by the propositions, calculations show that Proposition 6.3 gives nothing of value; the bound is greater than p for any $0 < p < 1/2$, so we gain no information over the bound of Theorem 4.5. On the other hand, the bound of Proposition 6.4 gives useful values (i.e., smaller than p) for p up to approximately 0.2.

ACKNOWLEDGMENTS

We are grateful to Moni Naor and Ron Holzman for their helpful comments and suggestions. We thank the anonymous referees, whose remarks have helped us improve our presentation.

Received September 9, 1994; final manuscript received June 18, 1995

REFERENCES

[AAC91] Ahamad, M., Ammar, M. H., and Cheung, S. Y. (1991), Multidimensional voting, *ACM Trans. Comput. Systems* **9**(4), 399–431.

[AE91] Agrawal, D., and El-Abbadi, A. (1991), An efficient and fault-tolerant solution for distributed mutual exclusion, *ACM Trans. Comput. Systems* **9**(1), 1–20.

[AS92] Alon, N., and Spencer, J. (1992), "The Probabilistic Method," Wiley, Chichester.

[Bec78] Beck, J. (1978), On 3-chromatic hypergraphs, *Discrete Math.* **24**, 127–137.

[BG86] Barbara, D., and Garcia-Molina, H. (1986), The vulnerability of vote assignments, *ACM Trans. Comput. Systems* **4**(3), 187–213.

[BG87] Barbara, D., and Garcia-Molina, H. (1987), The reliability of vote mechanisms, *IEEE Trans. Comput.* **C-36**, 1197–1208.

[BI95] Bioch, J. C., and Ibaraki, T. (1995), Decompositions of positive self-dual Boolean functions, *Discrete Math.* **140**, 23–46.

[Bol86] Bollobás, B. (1986), "Combinatorics," Cambridge Univ. Press, Cambridge, UK.

[BP75] Barlow, R. E., and Proschan, F. (1975), "Statistical Theory of Reliability and Life Testing," Holt, Rinehart & Winston, New York.

[BPT89] Borland, P. J., Proschan, F., and Tong, Y. L. (1989), Modelling dependence in simple and indirect majority systems, *J. Appl. Probab.* **26**, 81–88.

[CAA90] Cheung, S. Y., Ammar, M. H., and Ahamad, M. (1990), The grid protocol: A high performance scheme for maintaining replicated data, *in* "Proc. 6th IEEE Int. Conf. Data Engineering," pp. 438–445.

[Che52] Chernoff, H. (1952), A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations, *Ann. Math. Statist.* **23**, 493–509.

[Coh93] Cohen, H. (1993), "Quorum Systems: Domination, Fault-Tolerance, Balancing," Master's thesis, Department of Applied Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot, Israel, 1993.

[Con] Condorcet, N. (1785), Essai sur l'application de l'analyse à la probabilité des decisions rendues à la pluralite des voix, Paris.

[DGS85] Davidson, S. B., Garcia-Molina, H., and Skeen, D. (1985), Consistency in partitioned networks, *ACM Comput. Surveys* **17**(3), 341–370.

[DKK+94] Diks, K., Kranakis, E., Krizanc, D., Mans, B., and Pelc, A. (1994), Optimal coteries and voting schemes, *Inform. Process. Lett.* **51**, 1–6.

[EKR61] Erdős, P., Ko, C., and Rado, R. (1961), Intersection theorems for systems of finite sets, *Quart. J. Math. Oxford* **12**(2), 313–320.

[EL75] Erdős, P., and Lovász, L. (1975), Problems and results on 3-chromatic hypergraphs and some related questions, *in* "Infinite and Finite Sets," Colloq. Math. Soc. János Bolyai, Vol. 10, pp. 609–627, North-Holland, Amsterdam.

[Erd63] Erdős, P. (1963), On a combinatorial problem I, *Nordisk Mat. Tidskrift* **11**, 5–10.

[FKG71] Fortuin, C. M., Kasteleyn, P. W., and Ginibre, J. (1971), Correlation inequalities on some partially ordered sets, *Comm. Math. Phys.* **22**, 89–103.

[Fu90] Fu, A. (1990), "Enhancing Concurrency and Availability for Database Systems," Ph.D. thesis, Simon Fraser University, Burnaby, B. C., Canada, 1990.

[GB85] Garcia-Molina, H., and Barbara, D. (1985), How to assign votes in a distributed system, *J. Assoc. Comput. Mach.* **32**(4), 841–860.

[Gif79] Gifford, D. K. (1979), Weighted voting for replicated data, *in* "Proc. 7th Symp. Oper. Sys. Princip.," pp. 150–159.

[Her84] Herlihy, M. P. (1984), "Replication Methods for Abstract Data Types," Ph.D. thesis, Massachusetts Institute of Technology, MIT/LCS/TR-319, 1984.

[HMP95] Holzman, R., Marcus, Y., and Peleg, D. (1995), Load balancing in quorum systems, *in* "Proc. 4th Workshop on Algorithms and Data Structures, Kingston, Ont., Canada."

[Hol93] Holzman, R. (1993), personal communication.

[IK93] Ibaraki, T., and Kameda, T. (1993), A theory of coteries: Mutual exclusion in distributed systems, *IEEE Trans. Parallel Distrib. Systems* **4**(7), 779–794.

[INK92] Ibaraki, T., Nagamochi, H., and Kameda, T. (1992), Optimal coteries for rings and related networks, *in* "Proc. 12th Inter. Conf. Dist. Comp. Sys., Yokohama, Japan," pp. 650–656.

[Kar68] Karlin, S. "Total Positivity," Vol. 1, Stanford Univ. Press, Stanford.

[KC91] Kumar, A., and Cheung, S. Y. (1991), A high availability $\sqrt{n}$ hierarchical grid algorithm for replicated data, *Inform. Process. Lett.* **40**, 311–316.

[KFYA93] Kakugawa, H., Fujita, S., Yamashita, M., and Ae, T. (1993), Availability of k-coterie, *IEEE Trans. Comput.* **42**(5), 553–558.

[KRS93] Kumar, A., Rabinovich, M., and Sinha, R. K. (1993), A performance study of general grid structures for replicated data, *in* "Proc. Inter. Conf. Dist. Comp. Sys."

[Kum91] Kumar, A. (1991), Hierarchical quorum consensus: A new algorithm for managing replicated data, *IEEE Trans. Comput.* **40**(9), 996–1004.

[Lov73] Lovász, L. (1973), Coverings and colorings of hypergraphs, *in* "Proc. 4th Southeastern Conf. Combinatorics, Graph Theory and Computing," pp. 3–12.

[Mae85] Maekawa, M. (1985), A $\sqrt{n}$ algorithm for mutual exclusion in decentralized systems, *ACM Trans. Comput. Systems* **3**(2), 145–159.

[MO79] Marshall, A. W., and Olkin, I. (1979), "Inequalities: Theory of Majorization and its Application," Academic Press, New York.

[MP92a] Marcus, Y., and Peleg, D. (1992), "Construction Methods for Quorum Systems," Technical Report CS92-33, The Weizmann Institute of Science, Rehovot, Israel.

[MP92b] Marcus, Y., and Peleg, D. (1992) "Load Balancing in Quorum Systems," Technical Report CS92-34, The Weizmann Institute of Science, Rehovot, Israel.

[MV88] Mullender, S. J., and Vitányi, P. M. B. (1988), Distributed match-making, *Algorithmica* **3**, 367–391.

[Nei92] Neilsen, M. L. (1992), "Quorum Structures in Distributed Systems," Ph.D. thesis, Dept. Computing and Information Sciences, Kansas State University, 1992.

[NM92] Neilsen, M. L., and Mizuno, M. (1992), Coterie join algorithm, *IEEE Trans. Parallel Distrib. Systems* **3**(5), 582–590.

[NW94] Naor, M., and Wool, A. (1994), The load, capacity and availability of quorum systems, *in* "Proc. 35th IEEE Symp. Found. of Comp. Science," pp. 214–225.

[NW95] Naor, M., and Wool, A. (1995), "Access Control and Signatures via Quorum Secret Sharing," Technical Report CS95-19, The Weizmann Institute of Science, Rehovot, Israel.

[Owe82] Owen, G. "Game Theory," 2nd ed., Academic Press, New York.

[PW93] Peleg, D., and Wool, A. (1993), "The Availability of Quorum Systems," Technical Report CS93-17, The Weizmann Institute of Science, Rehovot, Israel.

[PW95] Peleg, D., and Wool, A. (1995), Crumbling walls: A class of practical and efficient quorum systems, *in* "Proc. 14th ACM Symp. Princip. of Dist. Comp., Ottawa, 1995," pp. 120–129.

[Rag88] Raghavan, P. (1988), Probabilistic construction of deterministic algorithms: Approximating packing integer programs, *J. Comput. System Sci.* **37**, 130–143.

[Ray86] Raynal, M. (1986), "Algorithms for Mutual Exclusion," MIT Press, Cambridge, MA.

[RST92] Rangarajan, S., Setia, S., and Tripathi, S. K. (1992), A fault-tolerant algorithm for replicated data management, *in* "Proc. 8th IEEE Int. Conf. Data Engineering," pp. 230–237.

[RT91] Rangarajan, S., and Tripathi, S. K. (1991), A robust distributed mutual exclusion algorithm, *in* "Proc. 5th Inter. Workshop on Dist. Algorithms," Lecture Notes in Computer Science, Vol. 579, pp. 295–308. Springer-Verlag, Berlin/New York.

[SB84] Spasojevic, M., and Berman, P. (1994), Voting as the optimal static pessimistic scheme for managing replicated data, *IEEE Trans. Parallel. Distrib. Systems* **5**(1), 64–73.

[Tho79] Thomas, R. H. (1979), A majority concensus approach to concurrency control for multiple copy databases, *ACM Trans. Database Systems* **4**(2), 180–209.

[Tuz85] Tuza, Zs. (1985), Critical hypergraphs and intersecting set-pair systems, *J. Combin. Theory Ser. B* **39**, 134–145.

[YG94] Yan, T. W., and Garcia-Molina, H. (1994), Distributed selective dissemination of information, *in* "Proc. 3rd Inter. Conf. Par. Dist. Info. Sys.," pp. 89–98.