SIAM J. DISCRETE MATH.
Vol. 15, No. 3, pp. 416–433

HOW TO BE AN EFFICIENT SNOOP, OR THE PROBE COMPLEXITY OF QUORUM SYSTEMS*

DAVID PELEG† AND AVISHAI WOOL‡

Abstract. 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.

When the elements may fail, a user of a distributed protocol needs to quickly find a quorum all of whose elements are alive or evidence that no such quorum exists. This is done by *probing* the system elements, one at a time, to determine if they are alive or dead.

This paper studies the *probe complexity* $\mathcal{PC}(\mathcal{S})$ of a quorum system $\mathcal{S}$, defined as the worst case number of probes required to find a live quorum or to show its nonexistence in $\mathcal{S}$, using the best probing strategy.

We show that for large classes of quorum systems, all n elements must be probed in the worst case. Such systems are called *evasive*. However, not all quorum systems are evasive; we demonstrate a system where $O(\log n)$ probes always suffice. Then we prove two lower bounds on the probe complexity in terms of the minimal quorum cardinality $c(\mathcal{S})$ and the number of minimal quorums $m(\mathcal{S})$. Finally, we show a universal probe strategy which never makes more than $c(\mathcal{S})^2 - c(\mathcal{S}) + 1$ probes; thus any system with $c(\mathcal{S}) \leq \sqrt{n}$ is nonevasive.

Key words. quorum systems, distributed computing, evasiveness, strong and simple games

AMS subject classifications. 68M14, 68Q25, 68R05, 91A10

PII. S0895480198343819

1. Introduction.

1.1. An illustrating scenario. The shareholders of the MegaBucks corporation need to vote on a decision with major implications. Due to a history of splits and merges, the voting structure is rather complicated, with many committees and subcommittees, often with a shareholder having a vote in many subcommittees. In game theory, such a voting structure is called a strong and simple game.

The reporter U.R. Nosey has the task of finding out whether the collective decision will be "yes" or "no." He can do this by asking the voters, one by one, how they plan to vote (assuming nobody lies or changes their mind after talking to the reporter). Mr. Nosey can stop his snooping when he finds a collection of voters with the same opinion that together can force the outcome, i.e., when he finds a winning coalition all of whose members will vote the same way.

The main questions that we address in this paper are the following: How should Mr. Nosey choose the next voter to ask each time so he can finish his task with the smallest number of conversations? How many voters must he ask under the worst possible configuration of answers? In particular, must he ask all the voters?

*Received by the editors August 24, 1998; accepted for publication (in revised form) April 24, 2002; published electronically June 5, 2002. An extended abstract of this paper appeared in *Proceedings of the Fifteenth ACM Symposium on Principles of Distributed Computing,* Philadelphia, PA, 1996, pp. 290–299.

http://www.siam.org/journals/sidma/15-3/34381.html

†Department of Applied Mathematics and Computer Science, The Weizmann Institute, Rehovot 76100, Israel (peleg@wisdom.weizmann.ac.il). This author's work was supported in part by grants from the Israel Science Foundation and from the Israel Ministry of Science and Art.

‡Department of Electrical Engineering—Systems, Tel Aviv University, Ramat Aviv 69778, Israel (yash@acm.org).

This game-theoretic scenario is analogous to the distributed systems scenario we have been dealing with all along. In the corresponding terminology, processors replace voters, winning coalitions are quorums, and the voting structure is the quorum system. The fact that the game is a strong and simple game is equivalent to the intersection property of a quorum system.

Any quorum-based distributed protocol must access, at some stage, a quorum all of whose processors are functioning. However, if processors may fail, then the protocol must *probe* the processors to determine if they are alive or dead, prior to using them. In the analogy with the snoopy reporter's problem, the processors' live/dead states correspond to the voters' individual decisions. Like the reporter, the protocol needs to probe processors one by one until a live quorum is found or until it is certain that no such quorum exists.

Clearly, it is desirable to probe as few processors as possible, since the number of probes measures the communication complexity of the distributed protocol. Therefore, in quorum system language, we are interested in the following questions: What strategy should be used to probe a given quorum system efficiently? How many probes are necessary in the worst failure configuration? In particular, is it true that all processors must be probed in the worst case? The maximal number of probes needed to determine if a live quorum exists is what we call the *probe complexity* of a quorum system $\mathcal{S}$ and is denoted by $\mathcal{PC}(\mathcal{S})$.

1.2. Related work. The rest of this paper uses the terminology of quorum systems. A good reference to game theory is [25]. Simple games, and their interpretations in reliability theory, are the subject of [29]. A discussion of the connection between strong and simple games and quorum systems can be found in [23].

Quorum systems serve as a basic tool providing a uniform and reliable way to achieve coordination between the processors and have been used in the study of problems such as *mutual exclusion* (cf. [30]), *data replication protocols* (cf. [6, 12, 36]), *distributed access control and signatures* (cf. [21]), and secure multiparty computation protocols (cf. [4]).

Many different quorum systems constructions appear in the literature. The simplest systems use *voting* to define the quorums [34, 10, 9]. Alternative constructions, which play a part in this paper, are found in [19, 7, 20, 1, 17, 13, 28].

Quorum systems, as tools for distributed protocols, were analyzed using various performance measures. The most widely studied measure is the availability (cf. [2, 26]). Other measures are the load [22] and load balancing [13]. A comprehensive analysis of all the above-mentioned quorum systems and some others can be found in [35].

The measure we call probe complexity is equivalent to the notion of the *argument complexity* of a boolean function, which is the maximum number of arguments of a boolean function f that must be tested in order to compute f. Aanderaa and Rosenberg conjectured that every nontrivial, monotone boolean function over n variables, describing a *graph property*, requires $\Omega(n)$ arguments to be tested in the worst case [32]. Karp conjectured that in fact every such property is *evasive*, i.e., requires that all n arguments be tested. The Aanderaa–Rosenberg conjecture was proved by Rivest and Vuillemin [31], who also showed that almost every boolean function is evasive for large n. Karp's stronger conjecture was later proved by [15].

To our knowledge, the probe complexity of quorum systems, or, equivalently, the argument complexity of boolean functions characterizing a quorum system, has not been studied before. In fact, most of the techniques of [31] and [15] are not applicable

in our case. This is since both proofs rely on the fact that a graph property P has a nice algebraic structure: the group of permutations of the k vertices acts transitively on the $n = \binom{k}{2}$ edges while preserving P. Boolean functions characterizing quorum systems rarely have such symmetry.

Following the appearance of our preliminary results in [27], Bazzi [3] introduced the related measure of cost-of-failures of a quorum system. This is the maximal number of probes that are needed per failure, which is essentially our probe complexity normalized by the number of failures that occurred.

1.3. New results. This paper addresses the question of how to quickly search for a live quorum in a distributed system when failures may occur, in the worst case model. Namely, we assume that an adversary, whose purpose is to force the user to make many probes, decides which elements fail.

After formalizing our model, we start with a discussion of evasiveness. We prove that large classes of quorum systems are evasive, including voting systems, crumbling walls, the finite projective plane, and compositions of these. However, and somewhat surprisingly, we show that not all quorum systems are evasive. We do this by demonstrating that the Nuc system of [7] requires only $O(\log n)$ probes in the worst case.

Next we prove two general lower bounds on the probe complexity of a quorum system in terms of combinatorial parameters of the system $\mathcal{S}$. We show that if the smallest quorum is of cardinality $c(\mathcal{S})$, then $\mathcal{PC}(\mathcal{S}) \geq 2c(\mathcal{S}) - 1$, and this bound is exactly tight for some examples. We also show that if $\mathcal{S}$ has $m(\mathcal{S})$ minimal quorums,[1] then $\mathcal{PC}(\mathcal{S}) \geq \log_2(m(\mathcal{S})) + 1$.

After these essentially negative results, we describe a more positive result. We give a universal probing strategy and prove an upper bound on the number of probes it makes in the worst case. We show that if all the quorums are of the same cardinality c (a uniform quorum system), then at most $c^2 - c + 1$ probes always suffice. As a corollary we obtain that every uniform quorum system with $c(\mathcal{S}) \leq \sqrt{n}$ is *not* evasive.

The organization of this paper is as follows. In section 2 we introduce the definitions and notation of quorum systems. In section 3 we introduce the probe model of a quorum system. In section 4 we prove that large classes of quorum systems are evasive, and we show an example of a nonevasive system. The two lower bounds we prove on the probe complexity appear in section 5. The universal strategy and its analysis are in section 6. Finally, the topic of probe complexity presents a number of significant problems which are still unresolved, and in section 7 we list several open questions and directions for further research.

2. Preliminaries.

2.1. Basic definitions.

DEFINITION 2.1. *A* set system $\mathcal{S} = \{S_1, \ldots, S_m\}$ *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 following* 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*. 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 $m(\mathcal{S})$, and the cardinality of the smallest quorum in $\mathcal{S}$ is denoted by $c(\mathcal{S}) = \min\{|S| : S \in \mathcal{S}\}$.

[1] A quorum S (of any cardinality) is called minimal if all its proper subsets $R \subset S$ are nonquorums.

DEFINITION 2.2. *Let $\mathcal{S}$ be a quorum system. $\mathcal{S}$ is* s-uniform *if $|S| = s$ for all $S \in \mathcal{S}$.*

DEFINITION 2.3. *A* Coterie *is a quorum system $\mathcal{S}$ that has the* minimality property: *there are no $S, R \in \mathcal{S}$ such that $S \subset R$.*

DEFINITION 2.4. *Let $\mathcal{R}, \mathcal{S}$ be coteries (over the same universe U). Then $\mathcal{R}$* 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 $R \subseteq S$. A coterie $\mathcal{S}$ is called* dominated *if there exists a coterie $\mathcal{R}$ such that $\mathcal{R} \succ \mathcal{S}$. If no such coterie exists, then $\mathcal{S}$ is* nondominated (ND). *Let* NDC *denote the class of all* ND *coteries.*

ND coteries are the "best" quorum systems in that they have the highest availability [26] and lowest load [22]. In what follows all the quorum systems are ND unless otherwise noted.

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

LEMMA 2.6 (see [9]). *Let $\mathcal{S} \in$ NDC, and let R be a transversal of $\mathcal{S}$. Then there exists a quorum $S \in \mathcal{S}$ such that $S \subseteq R$.*

Given an ND quorum system $\mathcal{S}$, we find it useful to count the transversals according to their cardinalities and to use the following combinatorial lemma.

DEFINITION 2.7. *Let $a_i^{\mathcal{S}}$ denote the number of size-i transversals of $\mathcal{S}$, i.e., the number of sets of size i that hit all the quorums of S for $0 \leq i \leq n$:*

$$a_i^{\mathcal{S}} = \big|\{X \in U : |X| = i \text{ and } \forall S \in \mathcal{S},\ S \cap X \neq \varnothing\}\big|.$$

The vector $a^{\mathcal{S}} = (a_0^{\mathcal{S}}, \ldots, a_n^{\mathcal{S}})$ is called the availability profile *of $\mathcal{S}$.*

LEMMA 2.8 (see [26]). *Let $\mathcal{S} \in$ NDC be given. Then $a_i^{\mathcal{S}} + a_{n-i}^{\mathcal{S}} = \binom{n}{i}$ for $0 \leq i \leq n$.*

An alternative view of a quorum system is that of a boolean function.

DEFINITION 2.9. *Let $\mathcal{S}$ be a quorum system. Let $x_1, \ldots, x_n$ be boolean variables corresponding to the elements of the universe. Then the* characteristic function *of $\mathcal{S}$ is $f_{\mathcal{S}} : \{0,1\}^n \to \{0,1\}$ defined by*

$$f_{\mathcal{S}}(x_1, \ldots, x_n) = \bigvee_{S \in \mathcal{S}} \bigwedge_{i \in S} x_i.$$

Clearly, $f_{\mathcal{S}}$ is monotone, and $f_{\mathcal{S}}(\mathbf{x}) = 1$ iff all the variables corresponding to some quorum have the value 1. Properties of characteristic functions of quorum systems are discussed extensively in [29, 14].

2.2. Examples. Let us illustrate the concept of quorum systems by giving some examples that play an important role in the results of this paper. The following constructions are all known to be ND coteries.

The majority system [34], denoted by Maj, is the collection of all sets of $\frac{n+1}{2}$ elements over a universe U when $n = |U|$ is odd.

The Wheel [13] contains $n-1$ "spoke" quorums of the form $\{1, i\}$ for $i = 2, \ldots, n$, and one "rim" quorum, $\{2, \ldots, n\}$.

In the finite projective plane (FPP) system of [20], $n = t^2 + t + 1$ for t which is a power of a prime. The quorums are all of size $t + 1$ and correspond to the lines of the projective plane.

The crumbling walls are a family of quorum systems due to [28]. The elements of a wall are logically arranged in *rows* of varying *widths*. A quorum in a wall is the union of one full row and a representative from every row below the full row. The

Wheel is a crumbling wall with two rows of width 1 and $n-1$. The triangular (Triang) system [19, 7] is another crumbling wall, in which row i has width i.

In the Tree system [1] the elements are organized in a complete rooted binary tree. A quorum in the system is defined recursively to be either (i) the union of the root and a quorum in one of the two subtrees or (ii) the union of two quorums, one in each subtree.

In the HQC system [17], the elements are the leaves of a complete ternary tree. The internal nodes are 2-of-3 majority gates.

The nucleus (Nuc) system of [7] 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 (call these "type A" quorums). Second, 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 $\mathcal{S}$. (These are "type B" quorums.)

3. The probe model. We assume that the elements (processors) of the system may occasionally fail. We assume that these failures are *crash* failures and that they are *detectable*. We also assume that the state of a processor does not change while the system is being probed; i.e., the processors are "fail-stop" [33]. We do not consider "lying" processors (Byzantine failures) or asynchronous communication with unbounded message delay.

When the protocol requires a user Alice to access a quorum, we assume that the configuration of failures is unknown to her. She can learn the configuration by *probing* the elements of the system one at a time (say by sending a message and waiting a timeout period for the reply). After probing element i, Alice knows if i is alive or dead.

Alice's task is to find a live quorum, or a witness that no such quorum exists, with the minimal number of probes. Note that if no live quorum exists, then the set R of dead elements comprise a transversal of the system $\mathcal{S}$. However, by Lemma 2.6 it follows that, for an ND system $\mathcal{S}$, R must contain some quorum S as a subset, all of whose elements are dead. Therefore Alice's stopping condition is symmetric for ND systems: find a quorum that contains only live elements or only dead elements.

We often refer to the live/dead state of the elements as a *coloring* of the universe U by calling a dead element "black" and a live element "white." Therefore Alice's task for an NDC system is as follows:

"Find a monochromatic quorum with the smallest number of probes."

We allow Alice to use an *adaptive strategy* to decide which element to probe next, based on the results of all the previous probes. We do not consider probabilistic strategies; i.e., Alice cannot flip coins. Therefore every probe strategy can be described by a rooted binary tree, with labels on the nodes (see Figure 3.1). A tree node labeled i represents a probe of element $i \in U$, and the first probe is to the element appearing at the root. The two outgoing edges from a node correspond to the probe results: the left edge is followed when i is alive, and the right edge when i is dead. The tree leaves represent stopping states for Alice and are colored black or white according to whether a live (white) quorum was found or a dead (black) one. Additionally, we attach the names of the found monochromatic quorums to the leaves (the witness quorums).

We are interested in the worst case number of probes that are necessary to guarantee the finding of a monochromatic quorum. Hence we have the following definition.

DEFINITION 3.1. *Let* $\mathcal{S} \in$ NDC *be a quorum system. Then the* probe complexity

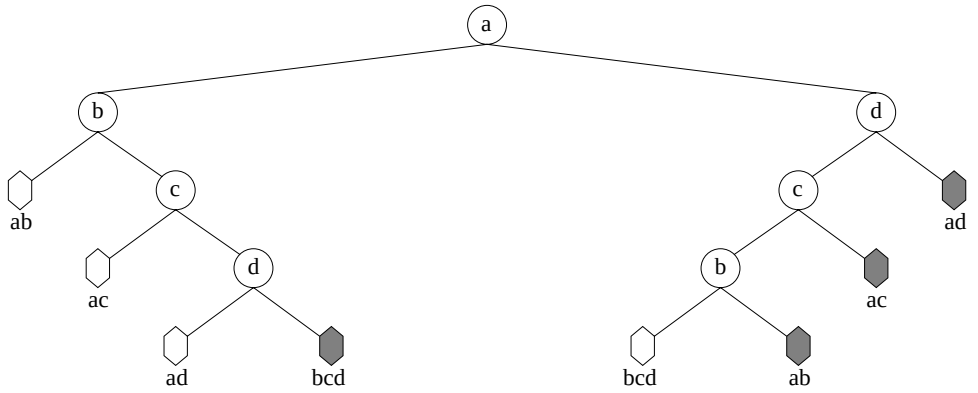

FIG. 3.1. *A possible probe strategy for the* Wheel_4 *system:* $\{\{\text{ab}\},\{\text{ac}\},\{\text{ad}\},\{\text{bcd}\}\}$. *Reaching a white hexagonal leaf indicates that a live quorum was found, and reaching a shaded one indicates a dead quorum. The names of the corresponding witness quorums appear below each leaf.*

of $\mathcal{S}$ *is*

$$\mathcal{PC}(\mathcal{S}) = \min_T\{depth(T)\},$$

where the minimum is taken over all possible probe strategy trees T*, and the depth is the number of nodes on the longest path from the root to a leaf in* T *(not counting the leaf itself).*

For example, the depth of the strategy shown in Figure 3.1 is 4, and it turns out that no strategy can do better, so $\mathcal{PC}(\text{Wheel}_4) = 4$. In fact, in what follows we show that $\mathcal{PC}(\text{Wheel})) = n$ for any universe size n. Such systems, which require all the elements to be probed (in the worst case) before a monochromatic quorum can be found, are especially important to us.

DEFINITION 3.2. *Let* $\mathcal{S}$ *be an* ND *quorum system over a universe of size* n*. If* $\mathcal{PC}(\mathcal{S}) = n$*, then we say that* $\mathcal{S}$ *is* evasive.

It is often useful to view Definition 3.1 as if Alice is playing a game against an *adversary* that controls the outcomes of the probes. The adversary knows Alice's strategy and has an unbounded computational power. The adversary's task is to force Alice to make as many probes as possible. Note that, since the adversary knows Alice's strategy, it can search the (possibly exponential sized) tree and find the deepest leaf and then choose a failure configuration that forces Alice to reach it. However, sometimes we can give explicit adversary strategies that do not exhaustively search Alice's strategy tree.

Evasiveness can be defined analogously for any boolean function f. Then a live element corresponds to a variable with value "1" and a dead element to a value "0." A function f is evasive if all n inputs need to be tested before the function can be evaluated, in the worst case. Saying that a quorum system $\mathcal{S}$ is evasive (as in Definition 3.2) is equivalent to saying that its characteristic function $f_{\mathcal{S}}$ is evasive as a boolean function (recall Definition 2.9).

4. Evasiveness. In this section we address the issue of evasiveness. Our starting point is the algebraic approach of [31], which we show to have limited usefulness in our case. Then in sections 4.2–4.5 we prove that large classes of quorum systems are evasive. Finally in section 4.6 we show that, surprisingly, there exist nontrivial quorum systems which are *not* evasive.

4.1. The algebraic approach. As part of their work on the evasiveness of graph properties, Rivest and Vuillemin [31] give in their Corollary 3.3 a sufficient condition for the evasiveness of a general monotone boolean function. Below we rephrase their result using our terminology to obtain a condition for quorum system evasiveness based on the availability profile (recall Definition 2.7).

PROPOSITION 4.1 (see [31]). *Let $a^{\mathcal{S}}$ be the availability profile of a quorum system $\mathcal{S} \in$ NDC. If*

$$\sum_{i \text{ even}} a_i^{\mathcal{S}} \neq \sum_{i \text{ odd}} a_i^{\mathcal{S}},$$

then $\mathcal{PC}(\mathcal{S}) = n$; i.e., $\mathcal{S}$ is evasive.

Example 4.2. The only FPP system [20] that is ND is the 7-point Fano plane [8]. For this system we have $a^{\text{FPP}} = (0, 0, 0, 7, 28, 21, 7, 1)$ by inspection, so the sum on the even indices is 35 while on the odd indices it is 29. Therefore by Proposition 4.1 the FPP system with $n = 7$ is evasive.

In their proof that almost all n-argument boolean functions f are evasive for large n, [31] in fact shows that the condition of Proposition 4.1 holds for all but an exponentially small fraction of the boolean functions. However, when we consider only the class NDC, the next proposition shows that Proposition 4.1 has limited usefulness.

PROPOSITION 4.3. *Let $\mathcal{S} \in$ NDC be over a universe of size $n = 2k$. Then*

$$\sum_{i \text{ even}} a_i^{\mathcal{S}} = \sum_{i \text{ odd}} a_i^{\mathcal{S}}.$$

Proof. Assume that k is odd. Note that, since n is even, if i is even, then so is $n - i$. Then using Lemma 2.8 and a combinatorial identity (cf. [16]) we obtain

$$\sum_{\substack{0 \le i \le n \\ i \text{ even}}} a_i^{\mathcal{S}} = \sum_{\substack{0 \le i < k \\ i \text{ even}}} \left(a_i^{\mathcal{S}} + a_{n-i}^{\mathcal{S}}\right) = \sum_{\substack{0 \le i < k \\ i \text{ even}}} \binom{n}{i} = \frac{1}{2} \sum_{\substack{0 \le i \le n \\ i \text{ even}}} \binom{n}{i} = 2^{n-2}.$$

However, a direct consequence of Lemma 2.8 is that $\sum a_i^{\mathcal{S}} = 2^{n-1}$. Therefore since the sum over the even indices is 2^{n-2} then so is the sum over the odd indices. The case where k is even is handled analogously. □

4.2. The adversary approach. An alternative method of proving that a quorum system is evasive is by giving an explicit strategy for an *oblivious* adversary that forces the user Alice to probe all n elements. An oblivious adversary is weaker than the adversary of Definition 3.1: it does not know Alice's strategy.

DEFINITION 4.4. *An* oblivious adversary strategy *is a procedure which computes the answer to a probe of any element $i \in U$, based only on the history of probes and answers.*

DEFINITION 4.5. *A quorum system $\mathcal{S}$ is called* obliviously evasive *if there exists an oblivious adversary strategy A which forces the user Alice to probe all n elements for any probing strategy she uses.*

An unbounded adversary, which knows Alice's strategy, can certainly simulate any oblivious adversary strategy. Therefore if a system $\mathcal{S}$ is obliviously evasive, then it is also evasive in the regular sense.

4.3. Composite systems. Our next goal is to prove Theorem 4.7, which allows us to prove the evasiveness of quorum systems that have a composite structure. For this purpose we use the characteristic function $f_{\mathcal{S}}$ of a quorum system, with the interpretation that $x_i = 1$ for a live element i and $x_i = 0$ otherwise. As we pointed out before, the evasiveness of the characteristic function is equivalent to the evasiveness of the quorum system.

LEMMA 4.6. *Let f be an obliviously evasive function. Then there exists an oblivious adversary strategy $A(\alpha)$ which ensures that f evaluates to $\alpha \in \{0,1\}$, and the decision between 0 and 1 is made after forcing Alice to make $n-1$ probes.*

Proof. By definition there exists an oblivious adversary strategy B which forces Alice to make n probes. Note that after making $n-1$ probes against B Alice cannot stop yet. Therefore there exist two configurations $\mathbf{x}_0$ and $\mathbf{x}_1$ that differ only in the value of the unprobed element i and that agree with the probe results on all other elements such that $f(\mathbf{x}_0) = 0$ and $f(\mathbf{x}_1) = 1$.

The strategy $A(\alpha)$ is the following. For the first $n-1$ probes return the answer given by strategy B. Suppose the answer given by B to the nth probe is b, which causes f to evaluate to β. If $\alpha = \beta$, then return b; otherwise, return $1-b$.

If β equals the desired output α, then the correctness of A is obvious. Otherwise, flipping the bit b changes the resulting configuration from $\mathbf{x}_0$ to $\mathbf{x}_1$, say, which in turn changes the output to α. ∎

THEOREM 4.7. *If $f(x_1, \ldots, x_t)$ is an obliviously evasive boolean function, and $\{g^j(y_1^j, \ldots, y_{n_j}^j)\}_{1 \le j \le t}$ is a family of t obliviously evasive functions on n_j variables, respectively, then the function*

$$f \circ \mathbf{g} = f(g^1(y_1^1, \ldots, y_{n_1}^1), \ldots, g^t(y_1^t, \ldots, y_{n_t}^t))$$

is obliviously evasive on $n = \sum_{1 \le j \le t} n_j$ variables.

Proof. Since f and $\{g^j\}_{1 \le j \le t}$ are all obliviously evasive, the adversary has strategies A_f and A_{g^j} that force Alice to probe all the inputs in each function separately. The composite adversary strategy is the following. When Alice probes an input y which belongs to some g^j in $f \circ \mathbf{g}$ then we have the following:

- If less than n_j of g^j's inputs were probed so far, return the answer given by A_{g^j} to the probe.
- If this is the n_jth probe of an input of g^j, then first activate the strategy A_f to determine the answer α for a probe of f's input x_j. Then activate $A_{g^j}(\alpha)$ and return the value that forces g^j to evaluate to α. (This can be done by Lemma 4.6.)

Since f is obliviously evasive, the use of strategy A_f ensures that the value of $f \circ \mathbf{g}$ remains undetermined until all the g^j functions are evaluated. (The evaluation of a function g^j is treated as a probe of the variable x_j of f.) Since the inputs sets of the g^j functions are disjoint, it is clear that all n_j inputs of each function must be probed before the value of g^j can be determined. ∎

Next we use Theorem 4.7 to prove (in Corollary 4.10) that the Tree and HQC systems are evasive. Proposition 4.9 serves as a building block for the proof.

DEFINITION 4.8. *A threshold "k-of-n" function is a boolean function on n variables that attains the value 1 iff at least k of its inputs have the value 1.*

PROPOSITION 4.9. *Every threshold "k-of-n" function is evasive.*

Proof. An adversary strategy $A(\alpha)$ which forces the user Alice to probe all n inputs is the following: Answer the first $k-1$ probes by "1." Answer the next $n-k$ probes by "0." Answer the nth probe by α. ∎

COROLLARY 4.10. *The Tree* [1] *and HQC* [17] *quorum systems are evasive.*

Proof. By Proposition 4.9 the 2-of-3 majority function is evasive. The HQC system is a complete ternary tree of 2-of-3 majorities, so by induction on the tree height and using Theorem 4.7 at each level it follows that HQC is evasive. A description of the Tree system as another tree of 2-of-3 majorities appears in [14], so a similar inductive proof shows its evasiveness. □

Remark. In fact, [14, 18] show that any NDC can be decomposed into a tree of 2-of-3 majorities. The Tree and HQC systems have decompositions that are *read-once*; i.e., each variable is input to a single 2-of-3 majority, so Theorem 4.7 can be used. However, in general, the decomposition is not read-once, so Theorem 4.7 cannot be applied.

4.4. Crumbling wall systems. Here we show another application of Theorem 4.7, which proves that the class of crumbling walls consists of evasive quorum systems.

PROPOSITION 4.11. *The Wheel quorum system is evasive.*

Proof. An adversary strategy $A(\alpha)$ which forces the user Alice to probe all n inputs is the following: If a rim element is probed during the first $n-2$ probes answer "0." If probe $n-1$ is to a rim element, and so were all the previous probes, then answer "1"; otherwise, answer "0." If the hub is probed during the first $n-1$ probes answer "1." Answer the nth probe by α.

If Alice probes the hub among her first $n-1$ probes, she will reach the nth probe, since the hub has value 1 and every known rim element has 0. Otherwise, she probes all $n-1$ rim element first to discover that they do not all have 0, so she must probe the hub as well. □

THEOREM 4.12. *Every crumbling wall quorum system is evasive.*

Proof. Informally, the adversary strategy is a variant of the following strategy: For any row i with n_i elements, answer the first $n_i - 1$ queries with "0"; answer the n_ith query with "1." It is not hard to see that this strategy forces Alice to make n probes. However, as stated the outcome is always "1," and so we need to modify strategy so that a "0" outcome is also possible. We now give a formal proof that this modified strategy is indeed an oblivious adversary strategy.

Consider a wall W on $d > 1$ rows, whose bottom row contains the elements $u_1, \ldots, u_{n_d}$, and let g_d be its characteristic function. Denote the characteristic function of the crumbling subwall on the top $d-1$ rows by g_{d-1}. Let $f(x_0, x_1, \ldots, x_{n_d})$ denote the characteristic function of the Wheel system on $n_d + 1$ variables, with variable x_0 corresponding to the hub. Then it is easy to see that the wall W can be decomposed into a Wheel whose hub is replaced by the top $d-1$ row subwall. Formally, $g_d = f(g_{d-1}, u_1, \ldots, u_{n_d})$. Thus we obtain a recursive decomposition of a crumbling wall using building blocks which are all Wheel systems and singletons on disjoint sets of elements. The Wheel system is evasive by Proposition 4.11, and singletons are trivially evasive, so we can apply Theorem 4.7 inductively and we are done. For the base of the induction, note that a crumbling wall with a single row is an n-of-n threshold system, so it is evasive by Proposition 4.9. □

4.5. Voting systems. Via the following definitions and lemmas we prove (in Theorem 4.18) that every quorum system defined by voting, which has no dummy elements, is evasive.

Notation. For a vector $v \in \mathbb{Z}^n$ and a set $S \subseteq U$, let $v(S) = \sum_{i \in S} v_i$.

DEFINITION 4.13. *Let $v \in \mathbb{Z}^n$ and an integer threshold T be given. The* voting system *$(v;T)$ is the collection of all the minimal sets $S \subseteq U$ such that $v(S) \geq T$:*

$$(v;T) = \{S \subseteq U : v(S) \geq T \text{ and } \forall u \in S,\ v(S \setminus \{u\}) < T\}.$$

Remark. A voting system is a quorum system (has the intersection property) iff the threshold $T > v(U)/2$. We need the more general definition for the proof of Theorem 4.18. However, with slight abuse of terminology we still refer to the sets of $(v;T)$ as "quorums."

The voting system with weights $(4,4,4,1)$ and threshold 7 is not evasive, since there is never any need to probe the element with weight 1. To avoid such trivialities we add the following definition.

DEFINITION 4.14. *Let $(v;T)$ be a voting system $v(U) = V$. An element $i \in U$ is a* dummy *if it does not belong to any (minimal) quorum, or, formally, $i \notin \cup\{S : S \in (v;T)\}$.*

DEFINITION 4.15. *Let $(v;T)$ be a voting system with $v(U) = V$. A* critical partition for *i is a partition $W|B$ of $U \setminus \{i\}$ into two sets W and B such that*

(1) *$v(W) < T$ and $v(W \cup \{i\}) \geq T$,*

(2) *$v(B) \leq V - T$ and $v(B \cup \{i\}) > V - T$.*

LEMMA 4.16. *Let $(v;T)$ be a voting system with $v(U) = V$. An element $i \in U$ is not a dummy in $(v;T)$ iff there exists a critical partition for i.*

Proof. ($\Rightarrow$) Assume that i is not a dummy. Then there exists a (minimal) quorum $S \in (v;T)$ such that $i \in S$. For this S, take $W = S \setminus \{i\}$ and $B = U \setminus S$. To prove (1), note that $v(W \cup \{i\}) = v(S) \geq T$ by definition, and $v(W) = v(S \setminus \{i\}) < T$ by the minimality of S. Now (1) implies (2), since $v(B) = v(U \setminus S) = V - v(S) \leq V - T$ and $v(B \cup \{i\}) = v(U \setminus W) = V - v(W) > V - T$.

($\Leftarrow$) Assume there exists a partition $W|B$ of $U \setminus \{i\}$ obeying (1) and (2). Take $R = W \cup \{i\}$. Then $v(R) = v(W \cup \{i\}) \geq T$ by (1). Now discard elements from R until it becomes a minimal set S for which $v(S) \geq T$ still holds. Then we claim that $i \in S$: Assume that i was discarded, then $v(S) \leq v(R \setminus \{i\}) = v(W) < T$, in contradiction to the definition of S. Hence $S \in (v;T)$ and $i \in S$, so i is not a dummy. ∎

LEMMA 4.17. *Let j be an element with the minimal weight v_j. If j is not a dummy in the voting system $(v;T)$, then $(v;T)$ is* dummy-free*; i.e., no element $i \in U$ is a dummy.*

Proof. Since j is not a dummy, there exists a minimal $S \in (v;T)$ such that $j \in S$. Consider some other element i. If $i \in S$ we are done, so assume otherwise. Take the set $R = S \setminus \{j\} \cup \{i\}$. Then $v(R) = v(S) - v_j + v_i \geq v(S) \geq T$, since v_j is the minimal weight. Now discard elements from R until a minimal set R' is obtained for which $v(R') \geq T$ still holds. We claim that $i \in R'$: otherwise, $v(R') \leq v(R \setminus \{i\}) = v(S \setminus \{j\}) < T$ by the minimality of S, in contradiction to the definition of R'. Hence $i \in R' \in (v;T)$ and i is not a dummy. ∎

THEOREM 4.18. *Every dummy-free voting system is evasive.*

Proof. For a voting system $(v;T)$, and a probe of element $i \in U$, the adversary uses the following oblivious strategy:

1. Let j be a minimal weight element in $U \setminus \{i\}$.
2. Find a critical partition $W|B$ for j.
3. If the probed element $i \in W$, then answer "white"; otherwise, answer "black."

Since $(v;T)$ is dummy-free, and in particular j is not a dummy, by Lemma 4.16 a critical partition $W|B$ can be found in step 2 for this j. Therefore the adversary's strategy is well defined.

After answering the probe of element i we obtain a new voting system $(v';T')$ on $U \setminus \{i\}$, with $v' = (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)$, and either $T' = T - v_i$ (if the answer was "white") or $T' = T$ (if the answer was "black"). Let $V' = v'(U \setminus \{i\}) = V - v_i$. Alice can stop probing in one of two cases:

- $T' \leq 0$. Then i completes a white quorum, so i must have been in W.
- $T' > V'$. Then no white quorum can be found, so i must have been in B.

Suppose that $i \in W$. However, $W|B$ is a critical partition for j, which was not probed yet and is outside W. So $T' = T - v_i \geq T - v(W) > 0$ by condition (1) of Lemma 4.16, and hence Alice cannot stop after a "white" answer. If $i \in B$, then, by condition (2) of Lemma 4.16, we get $V' = V - v_i \geq V - v(B) \geq V - (V - T) = T'$, so Alice cannot stop after a "black" answer either.

We still need to show that $(v';T')$ is dummy-free, and then the proof is complete by induction on the universe size n. Assume that $i \in W$. Since $W|B$ was critical for j, after answering the probe on i the partition $W \setminus \{i\}|B$ is clearly still critical for j (in the universe $U \setminus \{i\}$). A similar situation occurs when $i \in B$. However, j is a minimal weight element in $(v';T')$, so by Lemma 4.17 it follows that the resulting voting system $(v';T')$ is also dummy-free, and we are done. □

Remark. Finding the critical partition in step 2 is an NP-hard problem, but we assumed that the adversary has unbounded power.

4.6. Nonevasive examples. All the examples we have seen so far are of evasive quorum systems. Furthermore, in [31] it is shown that almost every boolean function on n variables is evasive for large n. Therefore it is reasonable to expect that, in a class of functions that has a "nice" structure, all the functions are evasive. This indeed is the case for graph-property functions, as shown by [31, 15]. However, for the class of ND quorum systems this is *not* the case. Below we show an ND uniform quorum system that has no dummy elements (i.e., every element belongs to some minimal quorum), which is not evasive.

Consider the Nuc system of [7] described in section 2.2. All its quorums are of size $c(\text{Nuc}) = r$, and it has $n = 2r - 2 + \frac{1}{2}\binom{2r-2}{r-1}$ elements, so $c(\text{Nuc}) \approx \frac{1}{2}\log_2 n$. The next proposition shows that in the Nuc system, $O(\log n)$ probes always suffice.

PROPOSITION 4.19. *$2r-1$ probes are always sufficient to find a monochromatic quorum in the* Nuc *system.*

Proof. Consider the following strategy. First probe the $2r-2$ elements of the nucleus. If at some stage r of these elements are found to have the same color—stop; a monochromatic quorum (of type A) was found.

The only configurations that require more probes are those in which the nucleus is partitioned into two sets of size $r-1$, T and T', of black and white elements, respectively. However, for every such partition there exists a unique element y outside the nucleus such that both $T \cup \{y\}$ and $T' \cup \{y\}$ are type B quorums. Therefore after probing this element y a monochromatic quorum will certainly be found. □

We shall see in section 6 that every uniform quorum system with $c(\mathcal{S}) \leq \sqrt{n}$ is nonevasive. However, is this condition sufficient? In fact, the question "do all nonevasive quorum systems have $c(\mathcal{S}) \leq \sqrt{n}$?" was left open in [27]. Here we answer this question in the negative, by showing a family of uniform ND quorum systems, with $c(\mathcal{S})$ ranging from $O(\log n)$ up to $n/2$, which are all nonevasive.

These systems are modifications of the Nuc system and are parameterized by a

number k. The Nuc(k) system has $2r-2$ nucleus elements and k satellite elements $b_0, \ldots, b_{k-1}$. All the sets of r nucleus elements are quorums (of type A) of Nuc(k). As for quorums of type B, we have the following rule. Enumerate the ways to partition the nucleus into two disjoint sets $T_j; T'_j$ with $|T_j| = |T'_j| = r-1$, using an index $j = 1, \ldots, \frac{1}{2}\binom{2r-2}{r-1}$. Then, for partition number j, the two corresponding type B quorums are $T_j \cup \{b_{j \pmod k}\}$ and $T'_j \cup \{b_{j \pmod k}\}$. In other words, Nuc($k$) is a Nuc system in which the satellite elements may appear in more than one pair of type B quorums.

FACT 4.20. Nuc(k) *is an ND, dummy-free, r-uniform quorum system for any* $1 \le k \le \frac{1}{2}\binom{2r-2}{r-1}$. *It has* $n = 2r-2+k$ *elements and* $m(\text{Nuc}(k)) = \frac{1}{2}\binom{2r}{r}$ *quorums.*

Remark. When $k = \frac{1}{2}\binom{2r-2}{r-1}$ then Nuc(k) $\equiv$ Nuc, so its minimal quorum size is $c(\text{Nuc}(k)) = r \approx \frac{1}{2}\log n$ as before. When $k = 1$ then Nuc(k) is precisely the Maj system over $n = 2r-1$ elements; i.e., $c(\text{Nuc}(1)) = (n+1)/2$.

PROPOSITION 4.21. $\mathcal{PC}(\text{Nuc}(k)) \le 2r-1$ *for all* $k \ge 1$.

Proof. The proof is identical to Proposition 4.19. □

COROLLARY 4.22. Nuc(k) *is nonevasive for all* $k \ge 2$.

5. Lower bounds. In this section we prove two lower bounds on the probe complexity, in terms of the smallest quorum size $c(\mathcal{S})$ and the number of quorums $m(\mathcal{S})$.

Notation. For a set R let $\mathbf{x}_R$ denote the configuration in which the elements of R are white and all others are black.

PROPOSITION 5.1. $\mathcal{PC}(\mathcal{S}) \ge 2c(\mathcal{S}) - 1$ *for any* $\mathcal{S} \in$ NDC.

Proof. First note that every correct strategy must probe at least $c(\mathcal{S})$ elements before stopping, regardless of the probe results, simply in order to probe all the elements of at least one quorum. Therefore the top $c(\mathcal{S})$ levels of any probe strategy tree are complete (see Figure 3.1).

Consider such a tree T, and consider L, its leftmost path from the root. By the above argument, L is at least $c(\mathcal{S})$ probes long. Let W be the set of elements labeling the top $c(\mathcal{S})-1$ nodes in L. There must exist a quorum $B \in \mathcal{S}$ such that $B \cap W = \varnothing$: otherwise, W is a transversal, which would imply that W contains a quorum by Lemma 2.6, contradicting the minimality of $c(\mathcal{S})$.

Now consider the configuration $\mathbf{x}_W$. On such a configuration, a user Alice using strategy T first probes all $c(\mathcal{S})-1$ elements of W and makes $c(\mathcal{S})-1$ left turns in her descent in the tree. At this point, no black element is encountered yet. However, the final decision must be black, since the quorum B is all black, so Alice must probe at least $c(\mathcal{S})$ more elements before reaching a black leaf. □

Remark. Equality holds in Proposition 5.1 in the following cases:

- In the Maj system, $c(\text{Maj}) = \frac{n+1}{2}$, and by Proposition 4.9 Maj is evasive, so $\mathcal{PC}(\text{Maj}) = n$.
- In the Nuc system with a nucleus of size $2r-2$ and $c(\text{Nuc}) = r$, Proposition 4.19 shows that $\mathcal{PC}(\text{Nuc}) \le 2r-1$, so Proposition 5.1 proves that in fact $\mathcal{PC}(\text{Nuc}) = 2r-1$.

PROPOSITION 5.2. $\mathcal{PC}(\mathcal{S}) \ge \log_2(m(\mathcal{S})) + 1$ *for any* $\mathcal{S} \in$ NDC.

Proof. Consider some probe strategy tree T. For each quorum $S \in \mathcal{S}$, let $\psi(S)$ be the (white) leaf in T which is reached when probing the configuration $\mathbf{x}_S$.

CLAIM 5.3. *Let* $S, R \in \mathcal{S}$. *If* $S \ne R$, *then* $\psi(S) \ne \psi(R)$.

Proof of the claim. Since $\mathcal{S} \in$ NDC it follows that $S \not\subseteq R$ and $R \not\subseteq S$. Let v be the first element in $(S \setminus R) \cup (R \setminus S)$ to be probed when the configuration is $\mathbf{x}_S$. Clearly, v is the first such element probed when the configuration is $\mathbf{x}_R$ as well. Assume w.l.o.g.

that $v \in S$. Then the path to $\psi(S)$ makes a left turn at v, since v is white in $\mathbf{x}_S$, but the path to $\psi(R)$ turns right at v, so $\psi(S) \neq \psi(R)$.

Claim 5.3 shows that ψ is a one-to-one mapping of quorums to white leaves of T; thus T has at least $m(\mathcal{S})$ white leaves. By swapping the roles of black and white and repeating the argument we obtain that T has at least $m(\mathcal{S})$ black leaves as well. Hence the depth of T is $\geq \log_2(2m(\mathcal{S}))$, which completes the proof of Proposition 5.2. □

Remarks. This lower bound is tight (up to additive constants) for the Maj and Nuc systems and is trivially exact for the singleton system. The bound is sometimes better than that of Proposition 5.1, as the following examples show.

- In the Tree system [1], $c(\text{Tree}) \approx \log n$ and $m(\text{Tree}) \approx 2^{n/2}$, so Proposition 5.2 gives a linear lower bound of $\mathcal{PC}(\text{Tree}) \geq n/2$, much better than that of Proposition 5.1 but still short of the truth which is $\mathcal{PC}(\text{Tree}) = n$ by Corollary 4.10.
- The Triang system [19] is uniform with $c(\text{Triang}) \approx \sqrt{2n}$ and $m(\text{Triang}) = \Omega((\sqrt{n})!)$. Thus Proposition 5.2 gives $\mathcal{PC}(\text{Triang}) \geq \Omega(\sqrt{n}\log n)$, which is better than the bound of Proposition 5.1 by a logarithmic factor but far from the true value $\mathcal{PC}(\text{Triang}) = n$ shown by Theorem 4.12 (since the Triang is a crumbling wall).

6. A universal probing strategy. In this section we give a universal probing strategy (see Figure 6.1) that works for any ND quorum system. We prove that $c^2 - c + 1$ probes always suffice for a c-uniform ND system when Alice uses this strategy. As a corollary we prove that any c-uniform ND quorum system with $c \leq \sqrt{n}$ is *nonevasive*.

Two probing strategies were described in [27] and [35], called the "alternating color" strategy and the "white" strategy. Both of these are special cases of the universal strategy, in which additional rules dictate some of the choices made. Thus the unified treatment here is more general and implies the results stated in [27, 35].

Moreover, as noted by Neilsen [24], the alternating color strategy of [27] is not well defined for dominated quorum systems. In contrast, the universal strategy we present here is well defined for all quorum systems (dominated or not), and as such it is a marked improvement over our earlier results.

The above-mentioned white strategy is similar to a procedure that was used in a very different context in [5], as part of the argument for proving that if $P \neq NP \cap co\text{-}NP$, then $P \neq NP \cap co\text{-}NP$ with a generic oracle. The exposition in [5] treats infinite languages and thus does not include the combinatorial analysis of the number of probes that we have here.

We need the following technical definition for the description of the strategy.

DEFINITION 6.1. *During the probing procedure, an element's color is either white, black, or unknown. A quorum $S \in \mathcal{S}$ is a* white candidate *(respectively,* black candidate*) if the colors of its elements are not all known and it has no black (respectively, white) elements.*

The strategy works in rounds. In every round the following steps are performed:

1. Pick candidate quorum S (either white or black) and probe all its unknown elements.
2. If a monochromatic quorum is found, stop.

FIG. 6.1. *The universal strategy.*

Remarks.

- The strategy probes all the elements of the candidate quorum S even if it becomes clear that S cannot be the solution. For instance, if S was a white candidate at the beginning of a round, then the strategy continues to probe the elements of S even after black elements are encountered.
- The strategy stops if *any* monochromatic quorum is found. Its color may well be different from that of the candidate picked for this round.
- A bichromatic quorum, which was discovered to have both white and black elements in previous rounds, is not a candidate any more.

LEMMA 6.2. *Let $\mathcal{S} \in$ NDC be given. If the universal strategy has not stopped by the end of round r, then both a white candidate and a black candidate still exist at the beginning of round $r+1$.*

Proof. Assume to the contrary that the strategy reaches round $r+1$ and a white candidate cannot be found. Then, by definition, every quorum has a (known) black element. Hence the set of black elements B is a transversal, and by Lemma 2.6 there exists some quorum $R \in \mathcal{S}$ for which $R \subseteq B$. However, this R is a monochromatic quorum, all of whose elements were probed. Therefore the strategy should have stopped after round r or earlier, in contradiction to the assumption that round $r+1$ was reached. The case of a missing black candidate is identical. □

Remark. Lemma 6.2 is incorrect for dominated systems. For example, consider the Star system $\{\{1,i\} : i = 2,\ldots,n\}$. If after the first round it turns out that element 1 is white and element 2 is black, then no black candidate quorum can be found for round 2.

DEFINITION 6.3. *Let $S_1, S_2, \ldots, S_r$ be the candidate quorums picked in the first r rounds. Let $B_i \subseteq S_i$ be the set of black elements in S_i* (the black part)*, and let $W_i \subseteq S_i$ be* the white part *for $1 \le i \le r$.*

LEMMA 6.4. *Assume that the strategy has not stopped by the end of round r. Let I_W and I_B be the sets of indices of the white and black candidates in the first r rounds, respectively. Then the black parts of the white candidates $\{B_i : i \in I_W\}$ are nonempty, disjoint sets and similarly for the white parts of the black candidates $\{W_j : j \in I_B\}$.*

Proof. If $B_i = \varnothing$ for some $i \in I_W$, then S_i is all white and the strategy should have stopped in round i, in contradiction to the assumption that a monochromatic quorum was not found up to round r.

Consider some $i \in I_W$. Note that S_i was a white candidate in round i, so at the beginning of the round all its known elements were white. Therefore $S_k \cap S_i \subseteq W_i$ for all $k < i$; thus S_i's black part B_i is disjoint from every previous candidate S_k. In particular it is disjoint from the black part of every previous white candidate. The proof for the white parts of black candidates is analogous. □

Remark. The quorum S_1 picked in round 1 is a black candidate and a white candidate simultaneously since all its elements' colors are unknown. All the subsequent quorums S_i are either white or black candidates, but not both, since $S_i \cap S_1 \neq \varnothing$ and the colors of all S_1's elements are known.

DEFINITION 6.5. *Let w_r and b_r denote the numbers of white and black candidate quorums picked in the first r rounds, respectively.*

LEMMA 6.6. *Assume the strategy has not stopped by the end of round r. Then*

- *if S_{r+1} is a white candidate, then the colors of at least b_r of its elements are known (to be white);*
- *if S_{r+1} is a black candidate, then the colors of at least w_r of its elements are*

known (to be black).

Proof. Assume S_{r+1} is a white candidate. This S_{r+1} intersects each of the b_r previous black candidates, so the intersections must be in the black candidates' white parts. However, the white parts of the black candidates are nonempty and disjoint by Lemma 6.4. Therefore S_{r+1} has at least b_r elements whose color is known (to be white) at the beginning of round $r+1$. The case of a black candidate is analogous. □

PROPOSITION 6.7. *Let $\mathcal{S} \in$ NDC be c-uniform. Then the universal strategy stops after probing at most c white candidates and at most c black candidates.*

Proof. To obtain a contradiction, assume that $b_r = c$ black candidates were probed by the end of round r, but the strategy had not stopped yet. Then by Lemma 6.2 a white candidate W still exists. By Lemma 6.6, c of W's elements are known to be white. However, $|W| = c$; thus W is already known to be monochromatic, in contradiction to the assumption that the strategy had not stopped. The argument for c white candidates is analogous. □

A direct application of Proposition 6.7 gives an upper bound of $\mathcal{PC}(\mathcal{S}) \leq 2c^2$. However, $2c^2$ is quite a rough estimate. A more careful analysis allows us to prove the tight bound of the next theorem.

THEOREM 6.8. *Let $\mathcal{S} \in$ NDC be c-uniform. Then $\mathcal{PC}(\mathcal{S}) \leq c^2 - c + 1$.*

Proof. Let P_i denote the aggregate number of probed elements by the end of round i, and let w_i and b_i be as in Definition 6.5. We prove that the following invariant holds.

CLAIM 6.9. *$P_i + (c - w_i)(c - b_i) \leq c^2 - c + 1$ for all rounds $i \geq 1$.*

Proof. The proof is by induction on i. For the induction base, recall that the quorum picked in round 1 is both a white candidate and a black candidate, so $w_1 = b_1 = 1$, and since $\mathcal{S}$ is c-uniform we have $P_1 = c$. So for $i = 1$ the invariant holds (with equality).

Now we assume the invariant holds for i and prove it holds for $i+1$. If a monochromatic quorum was found in round i, then the strategy stops and we are done. Otherwise, assume that the picked candidate S_{i+1} is white. By Lemma 6.6 we see that S_{i+1} has at least b_i elements whose color is known (to be white) at the beginning of round $i+1$. Hence at most $c - b_i$ elements are probed in round $i+1$ and

$$P_{i+1} \leq P_i + (c - b_i).$$

As remarked after Lemma 6.4, since S_{i+1} is a white candidate it cannot be a black candidate simultaneously. So $w_{i+1} = w_i + 1$ and $b_{i+1} = b_i$. Using the induction hypothesis we obtain that

$$\begin{aligned} P_{i+1} + (c - w_{i+1})(c - b_{i+1}) &\leq P_i + (c - b_i) + (c - w_i - 1)(c - b_i) \\ &= P_i + (c - w_i)(c - b_i) \\ &\leq c^2 - c + 1, \end{aligned}$$

and the invariant holds. The proof is analogous if S_{i+1} is a black candidate. This concludes the proof of Claim 6.9. □

By Proposition 6.7 we have that the strategy stops after some $r \leq 2c$ rounds, at which time $w_r \leq c$ and $b_r \leq c$. For this r we have from the invariant of Claim 6.9 that

$$P_r \leq c^2 - c + 1 - (c - w_r)(c - b_r) \leq c^2 - c + 1,$$

and thus $\mathcal{PC}(\mathcal{S}) \leq c^2 - c + 1$. □

COROLLARY 6.10. *Let $\mathcal{S} \in$ NDC be c-uniform. If $c \leq \sqrt{n}$, then $\mathcal{S}$ is nonevasive.*

Remarks.

- Theorem 6.8 is exactly tight for the 7-element FPP system: every FPP with quorums of size c has $n = c^2 - c + 1$, and the 7-element system (the only ND one) is evasive by Example 4.2.
- Corollary 6.10 is a sufficient condition for nonevasiveness, but it is not necessary. The Nuc(k) systems of section 4.6 are all c-uniform ND quorum systems which are nonevasive, but some of them have $c(\mathcal{S}) > \sqrt{n}$. In fact, for the Nuc($k$) systems Theorem 6.8 is not tight; the bound is $\approx c^2$, while $\approx 2c$ probes suffice by Proposition 4.19.

7. Concluding remarks and open questions. To the best of our knowledge, the question of how to search for a live quorum has not been addressed before in the context of distributed systems. We have demonstrated that the question is not a trivial one, especially when the system is defined by a combinatorial construction (rather than by voting). We believe that finding a good answer, in the form of a probing strategy and an analysis showing that it behaves "well," is an important and interesting goal. Here we list some of the related open problems we are interested in.

- Perhaps the most interesting problem, from a practical point of view, is the *average case* analysis of probing strategies, i.e., when the configuration of failures is not determined by a malicious adversary but is chosen probabilistically. Our initial results in this direction provided some evidence that the behavior is qualitatively different from the worst case. For instance, the Wheel system is evasive, but there is a trivial strategy for which the average number of probes is ≈ 3 for any universe size n. This direction was studied further in [11], which presented upper and lower bounds for the deterministic average case probe complexity of quorum systems in some classes of ND coteries, including majority, crumbling walls, Tree, Wheel and hierarchical quorum systems.

  A related problem concerns the probe complexity of *randomized* algorithms. This direction was also studied in [11], where it is shown that randomized algorithms may in many cases enjoy improved probe complexity in the worst case model compared to that achieved by deterministic ones.
- The universal strategy offers a large degree of freedom in choosing the candidate quorums—can this be used? An obvious rule would be to choose the candidate with the smallest number of elements whose color is unknown—does this (provably) help?
- Give a good probing strategy for nonuniform quorum systems. Note that our analysis of the universal probing strategy is essentially a "competitive analysis" with a competitive ratio of $c-1+1/c$ for uniform systems. However, for nonuniform systems we must replace c with $c_{\max}$, the maximal quorum cardinality, and in nonuniform systems typically $c_{\max} = \Omega(n)$.
- Everyday intuition tells us to probe the elements according to their relative influence. Can game-theory measures of influence such as the Shapley value or the Banzhaf index be used to devise a provably good strategy? Recently, Neilsen has provided anecdotal evidence supporting this intuition: In [24] he showed that for the Wheel system over four elements, probing in an order dictated by a dynamically decreasing Banzhaf index gives a better *average* probe complexity than that of a particular fixed strategy. However, proving

that this is a general phenomenon for all quorum systems, either in the worst case or in the average case, is still an open problem.

Acknowledgments. We are grateful to Moni Naor for many stimulating discussions, and in particular for pointing out the connection between our probing strategies and [5]. We thank Jean-Claude Bermond for his help in constructing examples that disproved some early conjectures.

REFERENCES

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

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

[3] R. A. Bazzi, *Planar quorums*, in Proceedings of the 10th International Workshop on Distributed Algorithms, Bologna, Italy, 1996, Lecture Notes in Comput. Sci. 1151, Springer-Verlag, Berlin, pp. 251–268.

[4] D. Beaver and A. Wool, *Quorum-based secure multi-party computation*, in Advances in Cryptology—EUROCRYPT'98, Espoo, Finland, 1998, Lecture Notes in Comput. Sci. 1403, K. Nyberg, ed., Springer-Verlag, Berlin, pp. 375–390.

[5] M. Blum and R. Impagliazzo, *Generic oracles and oracle classes*, in Proceedings of the 28th IEEE Symposium on Foundations of Computer Science, 1987, pp. 118–126.

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

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

[8] A. Fu, *Enhancing Concurrency and Availability for Database Systems*, Ph.D. thesis, Simon Fraser University, Burnaby, BC, Canada, 1990.

[9] H. Garcia-Molina and D. Barbara, *How to assign votes in a distributed system*, J. ACM, 32 (1985), pp. 841–860.

[10] D. K. Gifford, *Weighted voting for replicated data*, in Proceedings of the 7th Annual ACM Symposium on Operating Systems Principles, Pacific Grove, 1979, ACM, New York, 1979, pp. 150–159.

[11] Y. Hassin and D. Peleg, *Average probe complexity in quorum systems*, in Proceedings of the 20th ACM Symposium on Principles of Distributed Computing, Newport, RI, 2001, pp. 180–189.

[12] M. P. Herlihy, *Replication Methods for Abstract Data Types*, Ph.D. thesis, Massachusetts Institute of Technology, MIT/LCS/TR-319, Cambridge, MA, 1984.

[13] R. Holzman, Y. Marcus, and D. Peleg, *Load balancing in quorum systems*, SIAM J. Discrete Math., 10 (1997), pp. 223–245.

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

[15] J. Kahn, M. Saks, and D. Sturtevant, *A topological approach to evasiveness*, Combinatorica, 4 (1984), pp. 297–306.

[16] D. E. Knuth, *The Art of Computer Programming, Vol.* 1*—Fundamental Algorithms*, Addison-Wesley, Reading, MA, 1968.

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

[18] D. E. Loeb, *The fundamental theorem of voting schemes*, J. Combin. Theory Ser. A, 73 (1996), pp. 120–129.

[19] L. Lovász, *Coverings and colorings of hypergraphs*, in Proceedings of the 4th Southeastern Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, FL, 1973, Utilitas Mathematica, Winnipeg, MB, Canada, 1973, pp. 3–12.

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

[21] M. Naor and A. Wool, *Access control and signatures via quorum secret sharing*, IEEE Trans. Parallel Distrib. Systems, 9 (1998), pp. 909–922.

[22] M. Naor and A. Wool, *The load, capacity and availability of quorum systems*, SIAM J. Comput., 27 (1998), pp. 423–447.

[23] M. L. Neilsen, *Quorum Structures in Distributed Systems*, Ph.D. thesis, Department of Computing and Information Sciences, Kansas State University, Manhattan, KS, 1992.

[24] M. L. Neilsen, *A dynamic probe strategy for quorum systems*, in Proceedings of the 17th International Conference on Distributed Computing Systems, IEEE Computer Society Press, Los Alamitos, CA, 1997, pp. 95–99.

[25] G. Owen, *Game Theory*, 2nd ed., Academic Press, New York, 1982.

[26] D. Peleg and A. Wool, *The availability of quorum systems*, Inform. and Comput., 123 (1995), pp. 210–223.

[27] D. Peleg and A. Wool, *How to be an efficient snoop, or the probe complexity of quorum systems*, in Proceedings of the 15th ACM Symposium on Principles of Distributed Computing, Philadelphia, PA, 1996, pp. 290–299.

[28] D. Peleg and A. Wool, *Crumbling walls: A class of practical and efficient quorum systems*, Distrib. Comput., 10 (1997), pp. 87–98.

[29] K. G. Ramamurthy, *Coherent Structures and Simple Games*, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1990.

[30] M. Raynal, *Algorithms for Mutual Exclusion*, MIT Press, Cambridge, MA, 1986.

[31] R. L. Rivest and J. Vuillemin, *On recognizing graph properties from adjacency matrices*, Theoret. Comput. Sci., 3 (1976), pp. 371–384.

[32] A. L. Rosenberg, *On the time required to recognize properties of graphs: A problem*, SIGACT News, 5 (1973), pp. 15–16.

[33] F. B. Schneider, *What good are models and what models are good?*, in Distributed Systems, S. Mullender, ed., ACM Press, New York, Addison-Wesley, Reading, MA, 1993, pp. 17–26.

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

[35] A. Wool, *Quorum Systems for Distributed Control Protocols*, Ph.D. thesis, Department of Applied Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot, Israel, 1996.

[36] A. Wool, *Quorum systems in replicated databases: Science or fiction?*, Bull. IEEE Technical Committee on Data Engineering, 21 (1998), pp. 3–11; also available online from http://www.research.microsoft.com/research/db/debull/.