The HalfLie Problem

Joel Spencer
Courant Institute of Mathematical Sciences
New York University
New York, New York 10012
E-mail: spencer@cims.nyu.edu

Catherine H. Yan*
Department of Mathematics
Texas A&M University
College Station, Texas 77843
E-mail: cyan@math.tamu.edu

Proposed running head: HalfLie Problem

*Research supported by NSF Grant DMS-0070574 and a Sloan Fellowship.

Abstract

In Ulam's game Paul tries to find one of n possibilities with q Yes-No questions, while responder Carole is allowed to lie a fixed number k of times. We consider an asymmetric variant in which Carole must say yes when that is the correct answer (whence the *halflie*). We show that the maximal $A_k(q)$ for which Paul wins has the asymptotic form

$$A_k(q) = 2^{q+k}k!q^{-k} + \Theta(2^q q^{-k-\frac{1}{2}}).$$

Key Words: Ulam's problem, Liar's Game, asymmetric packing, asymptotic formula

Corresponding Author:
Catherine H. Yan
Department of Mathematics, Texas A&M University, College Station, TX 77843-3368
E-mail: cyan@math.tamu.edu
Fax: (979)-845-6028

1 Introduction

The basic liar game has two players whom we call Paul and Carole and three integer parameters (n, q, k). Paul is trying to find an unknown $x \in \{1, \ldots, n\}$ by asking q questions of Carole. The questions must all be of the form "Is $x \in A$?", where A is a subset of $\{1, \ldots, n\}$. Carole, the responder, is allowed to lie; however, she may lie at most k times. Paul wins if at the end of the q questions and responses the answer x is known with certainty.

Carole is allowed to play (and *will* play) an adversary strategy. That is, she does not preselect a particular x, but rather answers questions in a manner consistent with at least one possible x. At the end of the game, if there are at least two answers x, x' still valid (i.e., for which Carole has lied at most k times) then Carole has won; otherwise Paul is the winner of the game.

We further note that Paul's questions may (and generally *will*) be adaptive. That is, Paul's choice of question depends on Carole's previous answers.

In this formulation we have a two person perfect information game; thus we know that for any given triplet (n, q, k) either Paul or Carole has a perfect strategy. The question is, which one? Due to monotonicity, it suffices to answer the following more explicit question: given q and k, what is the maximal n (which we will denote by $A_k^*(q)$) for which Paul has a winning strategy?

Much work on the basic liar game was inspired by comments in the autobiography of Stanislas Ulam [10]. For this reason we, like many other authors, refer to the liar game as Ulam's game. The recent survey article by Pelc [6], which covers this game and many variants, with numerous references, is highly recommended. Early references include work by Alfred Rényi [7] and Elwyn Berlekamp [2]. Pelc [5] solved the problem completely when $k = 1$. Spencer [8] solved the problem completely for any fixed k with q sufficiently large. In particular, it is known that for any fixed k

$$A_k^*(q) \sim \frac{2^q}{\binom{q}{k}}, \tag{1}$$

where the asymptotics are as $q \to \infty$.

In this paper we modify Carole's ability to lie: she is still allowed to lie at most k times, but she is *only* allowed to lie when the truthful answer is "No". In other words, for Paul, any "No" he hears is a truthful answer and thus completely trustworthy; and any "Yes" answer he hears is a potential lie. As before, Carole can and will play an adversary strategy.

We call this the *halflie* game. We shall set $A_k(q)$ equal to the maximal n such that Paul has a winning strategy in the halflie game with parameters (n, q, k). F. Cicalese and D. Mundici [3] proved

$$A_1(q) \sim \frac{2^{q+1}}{q}. \tag{2}$$

This was proven independently by I. Dumitriu and J. Spencer [4] who showed more generally that

$$A_k(q) \sim \frac{2^{q+k}}{\binom{q}{k}} \tag{3}$$

for any fixed k. Our result here is a more accurate bound on $A_k(q)$:

Theorem 1.1. *Let $k \geq 1$ be an arbitrary positive integer. There exist positive constants c_1, c_2 such that for all sufficiently large q*

$$\frac{2^{q+k}}{\binom{q}{k}} + c_1 2^q q^{-k-\frac{1}{2}} < A_k(q) < \frac{2^{q+k}}{\binom{q}{k}} + c_2 2^q q^{-k-\frac{1}{2}}.$$

We emphasize that all of our asymptotic results are for k an arbitrary but fixed positive integer and q approaching infinity.

2 Two Formulations

We shall give two equivalent formulations of the halflie game, which are quite different in nature. Indeed, it has proven quite helpful to be able to regard the game in both of these respects.

2.1 Vectors

The state of the game in any middle position will be regarded as a vector $\vec{x} = (x_0, \ldots, x_k)$. Here x_i will represent the number of possibilities for which Carole has already made i lies. The initial position would then be $(n, 0, \ldots, 0)$. A query – is $x \in A$? – corresponds to a vector $\vec{a} = (a_0, \ldots, a_k)$ where a_i is the number of possibilities in A for which Carole has already made i lies. Paul's query may correspond to any $\vec{a}$ with integer coefficients and $\vec{0} \leq \vec{a} \leq \vec{x}$, where $\leq$ is defined coordinatewise. Let $YES(\vec{x}, \vec{a})$ denote the new position if Carole replies yes and $NO(\vec{x}, \vec{a})$ denote the new position if Carole replies no. A no reply must be the truth so that $NO(\vec{x}, \vec{a}) = \vec{x} - \vec{a}$. A yes reply, however, may be a lie. For $0 \leq i \leq k-1$ the $x_i - a_i$ possibilities for which Carole had lied i times would now have $i+1$ lies. The new position $YES(\vec{x}, \vec{a}) = (z_0, \ldots, z_k)$ with $z_0 = a_0$ and $z_{i+1} = a_{i+1} + x_i - a_i$ for $0 \leq i < k$. At the completion of the q rounds Paul has won if there is precisely one possibility left. That is, Paul wins if the final state $\vec{x}$ has one coefficient one and the rest zero. Note that it is illegal for Carole to play such that the final state is $\vec{0}$.

It is natural to extend the halflie game to arbitrary starts. Let $\vec{x} = (x_0, \ldots, x_k)$ with all $x_i \geq 0$, all x_i integral, and some x_i positive. The $(\vec{x}, q)$ halflie game begins with position $\vec{x}$ and has q rounds as defined above. In the original game format we may interpret this as beginning with $x_0 + \ldots + x_k$ possibilities, where there are x_i possibilities for which Carole is permitted to lie at most $k - i$ times.

2.2 Packing

We shall reformulate the evaluation of $A_k(q)$ as a packing problem. This approach is taken from [4]. The key notion is that of an i-set. This notion, as we shall see, captures the set of possible response sequences Carole can give with a particular value. For $0 \leq i \leq k$ an i-set is defined as a $P \subset \{Y, N\}^q$ together with some additional structure. P has a rooted tree structure, a tree with depth at most i. To each $w \in P$ is associated a set

$S(w) \subseteq \{1, \ldots, q\}$, called the lie positions of w. The $w \in P$ at depth j have $|S(w)| = j$. In particular, the root w has $S(w) = \emptyset$. We adapt a useful abuse of notation:

Definition 1. $\max(\emptyset) = 0$. *For* $S \neq \emptyset$, $\max(S)$ *denotes the maximal element of* S.

An i-set P can be defined recursively. The root is an arbitrary word in $\{Y, N\}^q$. Now let $w = w_1 \cdots w_q \in P$ be a word at level $j < i$ with the set of lie positions $S(w)$. Let $u > \max(S(w))$ with $w_u = N$. (Note that when $S(w) = \emptyset$ the first condition automatically applies.) Then there is a $w' = w'_1 \cdots w'_q \in P$ with the following properties.

1. w, w' agree on the first $u - 1$ coordinates,
2. $w'_u = Y$,
3. $S(w') = S(w) \cup \{u\}$,
4. w' is a child of w in the rooted tree structure.

Note that no conditions are placed on w'_i for $i > u$. We further require that for each such coordinate u there is precisely one such w' and that these are the only children of w in the rooted tree.

To better illustrate the definition above, we insert Fig. 1, which is a 2-set P in $\{Y, N\}^5$, consisting of words $NYNNY$, $YNYYN$, $NYYNY$, $NYNYN$, $YYNNY$, $YNYYY$, $NYYYN$ and $NYNYY$. It is drew as a rooted tree, in which for each $w \in P$, the lie positions of w are shaded.

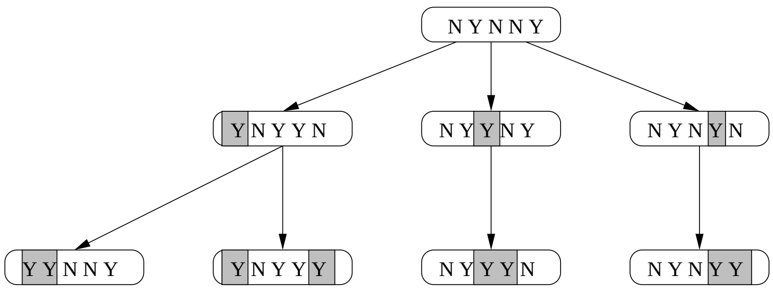

Figure 1: A 2-set in $\{Y, N\}^5$

We observe that a 0-set is an arbitrary singleton $P = \{w\}$. We further observe that the sizes of i-sets P can vary considerably. The smallest size is one, taking $w = Y \cdots Y$ as the root. The maximal size is $\sum_{j=0}^{i} \binom{q}{j}$, since the sets $S(w)$ are necessarily distinct. A 1-set has size $1 + l$ where l is the number of Ns in the root w.

We call a family of sets $P_\alpha \subseteq \{Y, N\}^q$ a packing if the P_α are pairwise disjoint.

Theorem 2.1. *Let* $\vec{x} = (x_0, \ldots, x_k)$. *Paul wins the* $(\vec{x}, q)$ *halflie game if and only if there exists a simultaneous packing of* x_i $(k - i)$*-sets in* $\{Y, N\}^q$.

Proof. Let Ω_i be disjoint sets with $|\Omega_i| = x_i$. Suppose Paul has a strategy to determine $\alpha \in \Omega = \cup \Omega_i$ where if $\alpha \in \Omega_i$, Carole may lie at most $k - i$ times. A strategy is a complete decision tree. We describe this tree by giving Paul's query in all circumstances. To every word $u \in \{Y,N\}^*$ of length less than q we correspond a set B_u. When the responses of Carole to date form the word u Paul asks if $\alpha \in B_u$. (Paul's first question, at the root of the decision tree, corresponds to u being the empty word.)

Fix such a strategy for Paul. For any $\alpha \in \Omega_i$ consider the set P_α of possible response sequences of Carole when the answer is α. Then $P_\alpha \subset \{Y,N\}^q$ must form a $(k-i)$-set. The root of P_α is the sequence Carole responds when always answering correctly. For each $w \in P_\alpha$ there is a set $S(w)$ of coordinates for which Carole has lied. When $|S(w)| < k-i$ and u is a position with $u > \max(S(w))$ and $w_u = N$, there must be another response sequences w'. This w' is identical with w for the first $u-1$ questions, but on the u-th round Carole makes one further lie. This corresponds precisely to the definition of the $(k-i)$-set. Since no response sequence can allow for the possibility of two distinct $\alpha, \beta \in \Omega$, it must be that P_α, $\alpha \in \Omega$ are distinct.

The converse also holds. Let Paul be given a family of disjoint P_α, $\alpha \in \Omega = \cup\Omega_i$, where P_α is a $(k-i)$-set if $\alpha \in \Omega_i$. Paul now creates a strategy. It is sufficient to define a set B_u for each $u \in \{Y,N\}^*$ of length less than q, (including the empty word), such that if the responses of Carole to date form the word u Paul asks if $\alpha \in B_u$. Let $u = u_1u_2\dots u_r$. The set B_u can be defined as follows. For each α Paul checks if u is the prefix for some $w^+ \in P_\alpha$ with $r+1 \notin S(w^+)$. If no such w^+ exists he can decide if $\alpha \in B_u$ arbitrarily. If such a w^+ exists and $w^+_{r+1} = Y$ then he puts α in B_u. If such a w^+ exists and $w^+_{r+1} = N$ then he puts α not in B_u.

With such defined B_u the set of possible response sequences of Carole when the answer is α is precisely P_α. To see this, let w be a response sequence of Carole. By the definition of B_u, if $w \in P_\alpha$, then α is a possibility at the end of the game. On the other hand, if $w \notin P_\beta$, then β can not be a possibility at the end of the game. Let $w' \in P_\beta$ be a word which has the longest common prefix $u = u_1 \dots u_r$ with w. (u may be the empty word.) Then $w_i = w'_i = u_i$ for $1 \le i \le r$, and $w_{r+1} \ne w'_{r+1}$. By the choice of w', either $w_{r+1} = N, w'_{r+1} = Y$ and $r+1 \notin S(w')$, or $w_{r+1} = Y, w'_{r+1} = N$ and $r+1 > S(w')$. In either cases w'_{r+1} is a truthful answer, and $r+1$ is not a lie position for w'. Hence Carole's answer w_{r+1} excludes β as a possibility.

As the P_α are disjoint at the end of the game there cannot be two distinct $\alpha, \beta \in \Omega$ that are both possibilities. $\square$

We close this section with a viewpoint which, although not formally a part of the proof, has given the authors a better understanding of the problem. We naturally define a random i-set P^i as follows. The root is uniformly chosen in $\{Y,N\}^q$. Let $w = w_1 \cdots w_q \in P$ be at level $j < i$, $u > \max(S(w))$ with $w_u = N$. Then w has child $w' = w_1 \cdots w_{u-1} Y w'_{u+1} \cdots w'_q$ where the w'_j, $u < j \le q$, are chosen independently and uniformly from $\{Y,N\}$. As the size of the random 1-set is simply one plus the number of N in the root we have $E[|P^1|] = 1 + \frac{q}{2}$. More generally

$$E[|P^i|] = \sum_{j=0}^{i} 2^{-j}\binom{q}{j}. \tag{4}$$

To show this, fix j and $1 \le u_1 < \dots < u_j \le q$. Let $I = I(u_1, \dots, u_j)$ be the indicator random variable for the existence of a chain $w^0, \dots, w^j$ of elements of P with w^0 the root and w^l differing first from w^{l-1} at position u_l. Then $E[I] = 2^{-j}$ as this occurs if and only if for each $1 \le l \le j$ the u_l-th position of w^{l-1} is an N, and these are selected uniformly. Further $|P^i| = 1 + \sum_{j=1}^{i} \sum I(u_1, \dots, u_j)$ since, other than the root, every element of P^i corresponds to a unique $j, u_1, \dots, u_j$. Equation (4) then follows from Linearity of Expectation. Asymptotically we note that

$$E[|P^i|] = 2^{-i}\binom{q}{i}(1 + \Theta(q^{-1})). \tag{5}$$

Paul wins from $(n, 0, \dots, 0)$ if and only if n k-sets can be packed into $\{Y, N\}^q$. If the k-sets were of average size the space used would be $nE[|P^k|]$ which would force $n \le 2^q/[E[|P^k|]]$. Note that this matches the result of (3) of Dumitriu and Spencer. Paul shall actually, as most clearly argued in Theorem 3.10, win with a somewhat larger n by using k-sets with size somewhat smaller than average.

3 Lower bounds

Here we give a strategy for Paul that wins the (n, q, k) halflie game when

$$n \le \frac{2^{q+k}}{\binom{q}{k}} + c_1 2^q q^{-k-\frac{1}{2}}, \tag{6}$$

where c_1 is a positive constant, depending only on k. The strategy will involve both the vector and the packing formats and is in three phases.

3.1 Phase I: Giving Ground

In the vector format the initial position is $\vec{x} = (n, 0, \dots, 0)$. Paul first gives ground and starts at the position $n\vec{1} = (n, n, \dots, n)$.

By the obvious monotonicity it suffices to show that Paul can win from this position. Some insight into why Paul has not given away too much is given in the next section.

3.2 Phase II: Near Perfect Splits

In the second phase Paul makes a series of near perfect splits, as defined below.

We begin by defining two linear transformations of R^{k+1} We set $P(x_0, \dots, x_k) = (z_0, \dots, z_k)$ with $z_0 = \frac{1}{2}x_0$, $z_1 = \frac{1}{2}x_1 - \frac{1}{4}x_0$ and, more generally, for $1 \le i \le k$

$$z_i = \frac{1}{2}x_i - \sum_{j=1}^{i} \frac{1}{2^{j+1}} x_{i-j}. \tag{7}$$

We set $L(x_0, \dots, x_k) = (y_0, \dots, y_k)$ with $y_0 = \frac{1}{2}x_0$, $y_1 = \frac{1}{2}x_1 + \frac{1}{4}x_0$ and, more generally, for $1 \le i \le k$

$$y_i = \frac{1}{2}x_i + \sum_{j=1}^{i} \frac{1}{2^{j+1}} x_{i-j}. \tag{8}$$

For convenience we also define a linear transformation

$$M(\vec{x}) = 2L(\vec{x}). \tag{9}$$

A simple calculation shows that if from position $\vec{x}$ Paul makes query $\vec{a} = P\vec{x}$ then Carole's response is immaterial,

$$YES(\vec{x}, P\vec{x}) = NO(\vec{x}, P\vec{x}) = L\vec{x}. \tag{10}$$

Indeed, $P\vec{x}$ was defined so as to have this property. On an intuitive level it seems natural that a play by Paul for which Carole's response is immaterial is a good play by Paul. If at position $\vec{x}$ Paul makes query $\vec{a} = P\vec{x}$ we call this a *perfect split.*

We shall be interested in series of perfect splits hence in the powers L^t. We are aided by the fact that, writing $L = (l_{ij})$ in matrix form, l_{ij} depends only on the difference $j - i$. Elementary linear algebra gives the formula

$$L^t(1, 0, \ldots, 0) = 2^{-t}M^t(1, \ldots, 0) = 2^{-t}(p_0(t), \ldots, p_k(t)), \tag{11}$$

where $p_0(t) = 1$, $p_1(t) = \frac{1}{2}t$ and, more generally,

$$p_i(t) = 2^{-i}\binom{t+i-1}{i}. \tag{12}$$

We further define $q_0(t) = 1$, $q_1(t) = 1 + \frac{1}{2}t$ and, more generally,

$$q_i(t) = \sum_{j=0}^{i} p_i(t). \tag{13}$$

The linear transformation L further satisfies

$$L^t(\vec{1}) = 2^{-t}M^t(\vec{1}) = 2^{-t}(q_0(t), \ldots, q_k(t)). \tag{14}$$

Let $\vec{z} = (z_0, \ldots, z_k)$. For all integers $t \geq 0$ we define the t-th weight function

$$W_t(\vec{z}) = \sum_{i=0}^{k} z_i q_{k-i}(t). \tag{15}$$

For any integer $t \geq 1$ and any $\vec{z}$

$$W_{t-1}(L\vec{z}) = \frac{1}{2}W_t(\vec{z}). \tag{16}$$

When the halflie game is at position $\vec{z}$ and there are t rounds remaining we shall say the game has weight function $W_t(\vec{z})$. Thus: *When Paul plays a perfect split the weight function halves.* We note the asymptotic formulae

$$p_i(t) = \frac{t^i}{2^i i!} + \Theta(t^{i-1}), \tag{17}$$

$$q_i(t) = \frac{t^i}{2^i i!} + \Theta(t^{i-1}) \tag{18}$$

hold for all $1 \le i \le k$ as $t \to \infty$. We further note that $L^0(\vec{1}) = \vec{1}$ so that $q_i(0) = 1$ for $0 \le i \le k$. Hence

$$W_0(\vec{z}) = z_0 + \ldots + z_k. \tag{19}$$

`Comments:` Paul will not, in general, be able to make a perfect split. The coefficients of $P\vec{x}$ might not be integral and the inequality $\vec{0} \le P\vec{x}$ might not be satisfied. (Note $P\vec{x} \le \vec{x}$ whenever $\vec{x} \ge \vec{0}$.) Still, suppose that beginning at $n\vec{1}$ Paul makes t perfect splits. The position after those t rounds would then be $L^t(n\vec{1}) = n2^{-t}M^t(\vec{1})$. We observe that when $n \sim 2^{q+k}k!q^{-k}$ then the q-th weight function $W_q(n\vec{1})$ is $\sim 2^q$. That is, were Paul to make q perfect splits from $n\vec{1}$ (which he actually would not be able to do) the resulting vector $\vec{z}$ would have $W_0(\vec{z}) = z_0 + \ldots + z_k \sim 1$. If $\vec{z}$ had only nonnegative integer coefficients it would have one coefficient one and the rest zero. That is, Paul would win the game. This provides, to our minds, an intuitive justification for the asymptotic formula for $A_k(n)$. It further gives some intuitive justification for the giving ground, replacing $(n, 0, \ldots, 0)$ by $(n, n, \ldots, n)$. Their q-th weight functions differ by a $1+O(q^{-1})$ factor. As our main result, Theorem 1.1, only attempts to bound $A_k(n)$ within a $1 + \Theta(q^{-1/2})$ bound this distinction would be inconsequential. Finally, we note that $q_i(q)$ is within a $1 + \Theta(q^{-1})$ factor of the expected size of a random i-set, given by Eqs. (4), (5). Thus the weight function $W_t(\vec{z})$ is close to (though not equal to!) the expected sum of the sizes of z_i randomly chosen $(k-i)$-sets in $\{Y, N\}^t$.

From position $\vec{x}$ we say that query $\vec{a}$ is a *near perfect split* if

$$|\vec{a} - P\vec{x}|_\infty \le \frac{1}{2}, \tag{20}$$

where $|\cdot|_\infty$ is the usual L^∞ norm, the maximal absolute value of the coefficients. Note that if $\vec{0} \le P\vec{x} \le \vec{x}$ then Paul always has a near perfect split by simply rounding off the coordinates of $P\vec{x}$. The following result will be used to show that the difference between perfect and near perfect splits is bounded by a constant. This difference shall be, for our work, asymptotically negligible.

Theorem 3.1. *Suppose from position $\vec{x}$ Paul plays a succession of near perfect splits. Let $\vec{x_t}$ denote the position after the t rounds. Then, regardless of Carole's responses*

$$|\vec{x_t} - L^t\vec{x}|_\infty \le 2^{k+1}. \tag{21}$$

Proof. This is immediate for $t = 0$, assume by induction it holds for t. We claim

$$|\vec{x}_{t+1} - L\vec{x_t}|_\infty \le 1. \tag{22}$$

If Paul's query were $P\vec{x_t}$ then we would have $\vec{x}_{t+1} = L\vec{x}_t$. Changing coordinates in the query by at most $\frac{1}{2}$ can change the coordinates in the new position by at most 1. (This occurs if, say, Paul lowers a_0 by $\frac{1}{2}$ and raises a_1 by $\frac{1}{2}$ and Carole says Yes. When Carole replies No the change in coordinates would be at most $\frac{1}{2}$.)

$$|\vec{x}_{t+1} - L^{t+1}\vec{x}|_\infty \le |\vec{x}_{t+1} - L\vec{x}_t|_\infty + |L(\vec{x}_t - L^t\vec{x})|_\infty. \tag{23}$$

We further note, examining the coefficients of the linear transformation L, that $|L\vec{y}|_\infty \leq (1-2^{-k-1})|\vec{y}|_\infty$ for any $\vec{y} \in R^{k+1}$. Thus

$$|\vec{x}_{t+1} - L^{t+1}\vec{x}|_\infty \leq 1 + (1-2^{-k-1})|\vec{x}_t - L^t\vec{x}|_\infty \leq 1 + (1-2^{-k-1})2^{k+1} \leq 2^{k+1}, \tag{24}$$

completing the induction. □

Theorem 3.2. *If $2^t \leq n2^{-2k-3}$ then Paul can make $t+1$ near perfect splits from initial position $n\vec{1}$*

Proof. It suffices to show that $P\vec{x}(r) \geq \vec{0}$ for $0 \leq r \leq t$, where $\vec{x}(r)$ is the position after r rounds. By Eq. (14), the position $\vec{x}(r)$ is $n2^{-r}(q_0(r), \ldots, q_k(r)) + \vec{E}_r$ with $|\vec{E}_r|_\infty \leq 2^{k+1}$. The i-th coordinate of $P\vec{x}(r)$ is

$$z_i = \frac{1}{2}x_i - \sum_{j=1}^{i} \frac{1}{2^{j+1}} x_{i-j} \geq n2^{-r}[\frac{1}{2}q_i(r) - \sum_{j=1}^{i} \frac{1}{2^{j+1}} q_{i-j}(r)] - 2^{k+1}. \tag{25}$$

As the $q_i(r)$ are increasing in i,

$$z_i \geq n2^{-r}2^{-i-2}q_i(r) - 2^{k+1} \geq n2^{-r}2^{-k-2} - 2^{k+1},$$

which is nonnegative for $0 \leq r \leq t$, by the hypothesis. □

The second phase begins in position $n\vec{1}$ and Paul makes a series of perfect splits. We shall end the second phase earlier than the above theorem allows - as the third phase shall be "better than perfect." To avoid trivialities we shall assume $n \geq 2^q q^{-k}$. Certainly increasing n only makes Paul's task harder.

Theorem 3.3. *Let $\epsilon > 0$ be fixed and arbitrarily small. For q sufficiently large (dependent on k, ϵ) and $n \geq 2^q q^{-k}$ Paul may make $\lceil (1-\epsilon)q \rceil$ perfect splits from initial position $n\vec{1}$.*

Proof. We simply check that for q sufficiently large, $t = \lceil (1-\epsilon)q \rceil$, and $n \geq 2^q q^{-k}$ we have $2^t \leq n2^{-2k-3}$. □

3.3 Phase III: Algebra

For $w \in \{Y, N\}^Q$ and $0 \leq i \leq k$ we define the *i-shadow* of w, written $P_i(w)$, as the set of all $w' \in \{Y, N\}^Q$ that may be reached from w (including w itself) by changing at most i coordinates which were N into Y. The i-shadows $P_i(w)$ are a special form of i-set. For any $w' \in P_i(w)$ the set $S(w')$ of lie positions is the set of coordinates where w, w' differ. For example, in Fig. 2 we include the 2-shadow of the word $NYNNY \in \{Y, N\}^5$, where for each word, the lie positions are shaded.

Suppose w has L coordinates $w_u = N$. Then

$$|P_i(w)| = \sum_{j=0}^{i} \binom{L}{j} \tag{26}$$

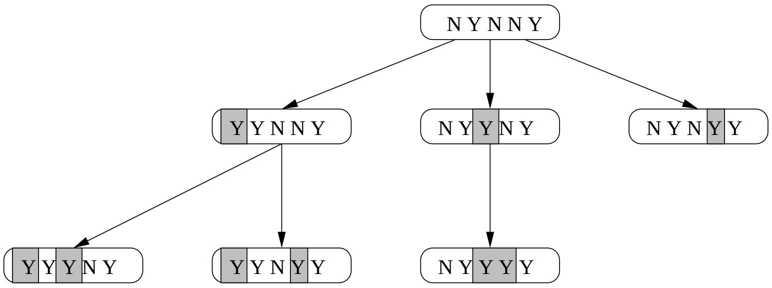

Figure 2: The 2-shadow $P_2(NYNNY)$

precisely. In application we shall set $L = \frac{Q}{2} - \Theta(\sqrt{Q})$. We are guided by noting that, for this L, $|P_i(w)|$ is $1 + \Theta(Q^{-1/2})$ times the expected size of the random i-set, as given by equations (4,5).

We associate $w \in \{Y, N\}^Q$ with a characteristic function $\chi_w : \{1, \ldots, Q\} \to \{0, 1\}$, setting $\chi_w(u) = 1$ if $w_u = N$ and $\chi_w(u) = 0$ if $w_u = Y$.

The following construction is the key to the third phase.

Theorem 3.4. *There is a constant Q_0 dependent only on k such that the following holds for all $1 \le i \le k$ and all $Q > Q_0$ with $Q + 1$ prime: Let $\alpha_1, \ldots, \alpha_i \in Z_{Q+1}$. Let $S = S(\alpha_1, \ldots, \alpha_i)$ be the set of $w \in \{Y, N\}^Q$ such that*

$$\sum_{u=1}^{q} \chi_w(u) u^j = \alpha_j \text{ for } 1 \le j \le i.$$

Then the i-shadows $P_i(w)$, $w \in S$, are disjoint.

Proof. Let $v = v_1 \cdots v_Q \in \{Y, N\}^Q$. Set

$$\sum_{u=1}^{q} \chi_v(u) u^j = \beta_j \text{ for } 1 \le j \le i. \tag{27}$$

For convenience, set $\gamma_j = \alpha_j - \beta_j$ for $1 \le j \le i$. Consider the following system of i equations in i unknowns $z_1, \ldots, z_i$ in the field Z_{Q+1}:

$$\sum_{s=1}^{i} z_s^j = \gamma_j \text{ for } 1 \le j \le i. \tag{28}$$

If $v \in P_i(w)$ and v is obtained from w by changing the $r_1, \ldots, r_l$ coordinates of w from N to Y then the above system has the solution $z_1 = r_1, \ldots, z_l = r_l$, $z_{l+1} = \ldots = z_i = 0$. (This includes the extremes $l = i$, no zeroes, and $l = 0$, so $v = w$ and all z's are zeroes.)

The above system of equations has been well studied. Over any field F of sufficiently high characteristic (dependent only on i) the system always has at most one solution, up to symmetry of the z_s. As the z_s determine w there can be at most one w. $\square$

For example, with $i = 2$ the equations $z_1 + z_2 = \gamma_1$, $z_1^2 + z_2^2 = \gamma_2$ give $z_1 z_2 = \frac{1}{2}[\gamma_1^2 - \gamma_2]$ and so z_1, z_2 must be the solutions z to the quadratic equation

$$z^2 - \gamma_1 z + \frac{1}{2}[\gamma_1^2 - \gamma_2] = 0 \tag{29}$$

unless the underlying field F has characteristic two. More generally, the first i elementary symmetric functions can be generated algebraically over the rationals from the first i functions $z_1^j + \ldots + z_i^j$. Explicitly, we have the following theorem.

Theorem 3.5. *Let e_j, p_j be the j-th elementary and power sum symmetric functions, respectively, i.e., $e_0 = p_0 = 1$,*

$$e_j = \sum_{i_1 < \cdots < i_j} z_{i_1} \cdots z_{i_j}, \qquad j \geq 1, \tag{30}$$

$$p_j = \sum_i z_i^j, \qquad j \geq 1. \tag{31}$$

Let $p_\lambda = p_{\lambda_1} p_{\lambda_2} \ldots$ if $\lambda = (\lambda_1, \lambda_2, \ldots)$. For a partition $\lambda = < 1^{m_1} 2^{m_2} \cdots >$, set $\epsilon_\lambda = (-1)^{m_2 + m_4 + \cdots} = (-1)^{n - \ell(\lambda)}$, ($\ell(\lambda)$ is the length of λ), and $c_\lambda = 1^{m_1} m_1! 2^{m_2} m_2! \cdots$. Then

$$e_j = \sum_\lambda \epsilon_\lambda c_\lambda^{-1} p_\lambda, \tag{32}$$

where λ ranges over all partitions of j.

This Theorem is well-known. For example, see Prop. 7.7.6. of [9].

Proposition 3.6. *The constant Q_0 in Theorem 3.4 can be taken as $k!$.*

Proof. As long as the characteristic of the underlying field F does not divide one of c_λ, where λ is a partition of i, $1 \leq i \leq k$, the $z_1, \ldots, z_i$ in (28) must then be the solutions to a unique polynomial over F of degree i, and hence is unique up to a symmetry of the z_s. As the prime factors of c_λ are bounded by k, it is sufficient to require $Q_0 = k!$. □

We note that for many $v \in \{Y, N\}^Q$ there will be no w with $v \in P_i(w)$. For w to exist first the system of equations must have a solution in Z_{Q+1}. Second, the nonzero z values of the solution must be such that the z-th coefficient of v is Y. Roughly speaking, a positive proportion of the v will lie in some $P_i(w)$. This proportion, however, is strictly less than one. Phase three, by itself, would only give a relatively weak lower bound on $A_k(n)$.

Theorem 3.7. *Let Q be sufficiently large (dependent only on k) with $Q + 1$ prime. Let $1 \leq i \leq k$. Let $0 \leq L \leq Q$ be integral. There exists a set $S_i \subseteq \{Y, N\}^Q$ such that*

1. *The i-shadows $P_i(w)$, $w \in S_i$, are disjoint.*
2. *All $w \in S_i$ have at most L coordinates $w_i = N$.*
3. *$|S_i| \geq (Q+1)^{-i} \sum_{u=0}^{L} \binom{Q}{u}$.*

Proof. For any $\alpha_1, \dots \alpha_i \in Z_{Q+1}$ the set of $w \in S(\alpha_1, \dots, \alpha_i)$ with at most L coordinates $w_i = N$ satisfies the first and second conditions. These sets are disjoint and their union is all w satisfying the second condition. One of these $(Q+1)^i$ sets $S(\alpha_1, \dots, \alpha_i)$ has size at least $(Q+1)^{-i}$ times the size of their union. $\square$

The above argument works for any $1 \le i \le k$ but not simultaneously for all $1 \le i \le k$. We achieve the simultaneity be using appropriate prefixes.

Theorem 3.8. *Let $p_1, \dots, p_k \in \{Y, N\}^T$ be such that the i-shadows $P_i(p_i)$ are mutually disjoint. Let $S_i \subseteq \{Y, N\}^Q$ be such that for each $1 \le i \le k$ the i-shadows $P_i(w)$, $w \in S_i$, are mutually disjoint. Set $R = Q + T$. Define $S_i^+ \subseteq \{Y, N\}^R$ to be the set of words $w^+ = p_i \circ w$, $w \in S_i$. Then the shadows $P_i(w^+)$ are disjoint over all $1 \le i \le k$, $w^+ \in S_i^+$.*

Proof. Consider $p_i \circ w$ and $p_j \circ w'$ and suppose $P_i(p_i \circ w)$ and $P_j(p_j \circ w')$ intersect. All elements of $P_i(p_i \circ w)$ begin with an element of $P_i(p_i)$ and all elements of $P_j(p_j \circ w')$ begin with an element of $P_j(p_j)$. Thus $i = j$ But then all elements of $P_i(p_i \circ w)$ end with an element of $P_i(w)$ and all elements of $P_i(p_i \circ w')$ end with an element of $P_i(w')$ so that $w = w'$. $\square$

The determination of the minimal T satisfying the conditions of the above theorem is an intriguing question to which we do not here contribute. For our purposes it shall suffice that there exists such a T. For definiteness, we set $T = 2 + \cdots + k$. We further let p_k be the word consisting of all Y's, and for $1 \le i < k$ let $p_i \in \{Y, N\}^T$ consist of $k+1$ coordinates N and the remainder Y, such that the different p_i have different coordinates equal N. Note that T depends only on k and so is, for our purposes, a constant. We remark, however, that the value of T very much affects the constant c_1 in our main result, Theorem 1.1.

Theorem 3.9. *Let Q be sufficiently large (dependent on k) such that $Q+1$ is a prime. Set $T = 2 + \cdots + k$ and $R = Q + T$. Let $0 \le L \le Q$. Let $\vec{z} = (z_0, \dots, z_k)$ be such that*

1. $z_i < (Q+1)^{-(k-i)} \sum_{u=0}^{L} \binom{Q}{u}$ *for* $0 \le i < Q$.
2. $$z_k + \sum_{i=0}^{k-1} z_i \left[\sum_{j=0}^{k-i} \binom{L+k}{j} \right] \le 2^R.$$

Then Paul wins the $(\vec{z}, R)$ halflie game.

Proof. Combining Theorems 3.7,3.8 we may, simultaneously for $0 \le i < k$, pack z_i $(k-i)$-shadows into $\{Y, N\}^R$ such that each root w^+ has at most $L+k$ coordinates N. (There are at most k from the prefixes $p_i \in \{Y, N\}^T$ and at most L from the suffixes $w \in \{Y, N\}^Q$.) Each $(k-i)$-shadow therefore has size at most $\sum_{j=0}^{k-i} \binom{L+k}{j}$. Thus the number of $w \in \{Y, N\}^R$ which are not in any of these shadows is at least z_k. But 0-shadows are *arbitrary* singletons $\{w\} \subset \{Y, N\}^R$. Thus we can further pack z_k 0-sets. $\square$

The above argument gives a critical advantage to Paul. In the application below we shall take L to be approximately $\frac{R-\sqrt{R}}{2}$. Roughly speaking, Paul packs the i'-shadows, $i' = k - i \neq 0$, into the "lower" region of $\{Y, N\}^R$, where the number of Ns is smaller than average and so the size of the i'-shadows is smaller than average. The singleton 0-sets then go in the remaining region, as their size is always one. He will, as we shall see, be able to pack more 0-sets since the i'-shadows, $i' \neq 0$, have taken up less space.

Theorem 3.10. *For all sufficiently small (dependent only on k) $\epsilon_1 < \epsilon_2$ there exists $c > 0$ so that the following holds for all sufficiently large $R = Q + T$ with $T = 2 + \ldots + k$ and $Q + 1$ prime: Let $\vec{z} = (z_0, \ldots, z_k)$ be such that*

1. $\epsilon_1 2^R < \sum_{i=0}^{k-1} z_i q_{k-i}(R) < \epsilon_2 2^R$,
2. $W_R(\vec{z}) := z_k + \sum_{i=0}^{k-1} z_i q_{k-i}(R) < 2^R(1 + cR^{-1/2})$.

Then Paul wins the $(\vec{z}, R)$ halflie game.

We note that some lower bound in the first condition is necessary as Paul cannot win when $z_0 = \ldots = z_{k-1} = 0$ and $z_k > 2^R$.

Proof. We shall show, for appropriate $\epsilon_1, \epsilon_2, c$, that the conditions of Theorem 3.9 are satisfied for sufficiently large R with

$$L = \lfloor \frac{1}{2}(R - \sqrt{R}) \rfloor. \tag{33}$$

Asymptotically (as $R \to \infty$), $Q = R - T = R - O(1)$ and $L = \frac{1}{2}(Q - \sqrt{Q}) + O(1)$. By the Central Limit Theorem

$$2^{-Q} \sum_{u=0}^{L} \binom{Q}{u} = \Pr[Bin[Q, \frac{1}{2}] \leq L] \to \Pr[N \leq -1], \tag{34}$$

where N is the standard normal. For $0 \leq i \leq k-1$

$$(Q+1)^{-(k-i)} \sum_{u=0}^{L} \binom{Q}{u} \sim R^{-(k-i)} 2^R [2^{-T} \Pr[N \leq -1]]. \tag{35}$$

The first condition implies $z_i q_{k-i}(R) < \epsilon_2 2^R$ so that

$$z_i < \epsilon_2 \frac{2^R}{q_{k-i}(R)} \sim \epsilon_2 2^R R^{-(k-i)} 2^{k-i} (k-i)!. \tag{36}$$

We shall require ϵ_2 sufficiently small so that

$$\epsilon_2 2^{k-i} (k-i)! < 2^{-T} \Pr[N \leq -1] \tag{37}$$

for $0 \leq i \leq k-1$. This insures that the first condition of Theorem 3.9 holds for R sufficiently large.

To show the second condition of Theorem 3.9, given the second condition of this theorem, it suffices to show

$$\sum_{i=0}^{k-1} z_i \Delta_{k-i}(R) > c2^R R^{-1/2}, \tag{38}$$

where we set, for $1 \le s \le k$,

$$\Delta_s(R) = q_s(R) - \sum_{j=0}^{s} \binom{L+k}{j}. \tag{39}$$

(Δ_s may be though of as the advantage of our algebraic construction over average s-sets.) Asymptotically (in R)

$$q_s(R) = \binom{R/2}{s}(1 + \Theta(R^{-1})), \tag{40}$$

whereas

$$\sum_{j=0}^{s} \binom{L+k}{j} = \binom{\frac{R-\sqrt{R}}{2} + O(1)}{s}(1 + \Theta(R^{-1})) = \binom{R/2}{s}(1 - R^{-1/2})^s(1 + \Theta(R^{-1})), \tag{41}$$

so that

$$\Delta_s(R) \sim sR^{-1/2} q_s(R) > (1 + o(1))R^{-1/2} q_s(R). \tag{42}$$

The lower bound of the first condition gives

$$\sum_{i=0}^{k-1} z_i \Delta_{k-i}(R) > (1 + o(1))R^{-1/2} \sum_{i=0}^{k-1} z_i q_{k-i}(R) > (1 + o(1))\epsilon_1 2^R R^{-1/2}, \tag{43}$$

and thus (38) is satisfied for any $c < \epsilon_1$ □

3.4 Synthesis

Paul's strategy is now easy to describe. To avoid technicalities we replace n by

$$n = \lfloor \frac{2^{q+k}}{\binom{q}{k}}(1 + c_1 q^{-1/2}) \rfloor. \tag{44}$$

First, Paul gives ground and starts at $n\vec{1}$. Second, Paul plays near perfect splits until there are some R rounds remaining in the game. Third, Paul applies Theorem 3.10 to win. R is the critical variable here, marking the time when Paul switches from the second to the third phase. If it is too small the conditions for the third phase will not yet apply and if it is too large the advantage of the third phase will not be sufficiently large. Further, $R - T + 1$ must be a prime and sufficiently large.

Recall that k, and hence $T = 2 + \cdots + k$ are fixed. Fix $\epsilon_1, \epsilon_2, c$ satisfying Theorem 3.10. Fix $\delta_1 < \delta_2$ with

$$1 - \epsilon_2 < (1 - \delta_2)^k < (1 - \delta_1)^k < 1 - \epsilon_1. \tag{45}$$

Select R so that

1. $\delta_1 q \le R \le \delta_2 q$,
2. $R - T + 1$ is prime.

We require here the classic result from Number Theory that for any positive γ there is a prime between n and $n(1+\gamma)$ for n sufficiently large. Applying this with $1+\gamma = \delta_2/\delta_1$, for q sufficiently large there will be a prime between $\delta_1 q - T + 1$ and $\delta_2 q - T + 1$ so that R will exist.

Since $W_q(n\vec{1}) \sim 2^q$, $W_R(\vec{z}) \sim 2^R$ where $\vec{z} = (z_0, \ldots, z_k) = L^{q-R}(n\vec{1})$. Further

$$z_k = n2^{R-q} q_k(q-R) \sim \frac{2^{q+k}}{\binom{q}{k}} 2^{R-q} \frac{(q-R)^k}{2^k k!} \sim 2^R \left(\frac{q-R}{q}\right)^k, \tag{46}$$

so that

$$(1 - (1-\delta_2)^k + o(1))2^R > W_R(\vec{z}) - z_k > (1 - (1-\delta_1)^k + o(1))2^R. \tag{47}$$

From Theorem 3.3 Paul applies near perfect splits for the first $q - R$ rounds, yielding a position $\vec{z}^* = (z_0^*, \ldots, z_k^*)$. From Theorem 3.1 all $|z_i - z_i^*| = O(1)$. Thus

$$|W_R(\vec{z}^*) - W_R(\vec{z})| = O(R^k) = o(2^R), \tag{48}$$

and

$$(1 - (1-\delta_2)^k + o(1))2^R > W_R(\vec{z}^*) - z_k^* > (1 - (1-\delta_1)^k + o(1))2^R. \tag{49}$$

For q (and hence R) sufficiently large

$$\epsilon_2 2^R > W_R(\vec{z}^*) - z_k^* > \epsilon_1 2^R. \tag{50}$$

Finally, we must choose c_1 for our main result, Theorem 1.1. As

$$W_q(n\vec{1}) = 2^q(1 + c_1 q^{-1/2}(1+o(1))), \tag{51}$$

we have

$$W_R(\vec{z}^*) = 2^R(1 + c_1 q^{-1/2}(1+o(1))) < 2^R(1 + c_1 \delta^{1/2} R^{-1/2}(1+o(1))). \tag{52}$$

Choose $c_1 > 0$ so that

$$c_1 \delta^{1/2} < c \tag{53}$$

with c the constant satisfying Theorem 3.10. Then for q sufficiently large we apply Theorem 3.10 and Paul succeeds in the third phase and wins the game.

4 Upper Bounds

For the upper bound we use the packing formulation, to show $A_k(q) < n$ we shall argue that n k-sets P cannot be packed in $\{Y, N\}^q$.

Definition 2. *When P is a k-set, $w, w' \in P$, w' a child of w, and u is the least integer with $w_u \ne w'_u$ we say w* spawns *w' at coordinate u.*

As a warm-up, and also as a guide to the full result, we give first the somewhat weaker bound. This result was proven in [4].

Proposition 4.1.

$$A_k(q) \le \frac{2^{q+k}}{\binom{q}{k}} \left(1 + O(q^{-1/2}\sqrt{\ln q})\right). \tag{54}$$

Proof. We call a word $w \in \{Y,N\}^q$ *rare* if it has fewer than $L = \frac{1}{2}(q - K\sqrt{q}\sqrt{\ln q})$ coordinates $w_i = N$, where K is a constant. Basic large deviation bounds (see, e.g., the appendix of [1]) give that the number of rare w is less than $2^q q^{-K^2/2}$. With $\frac{K^2}{2} > k + \frac{1}{2}$, the number is $o(2^q q^{-k-\frac{1}{2}})$ so that the number of k-sets in the packing that contain any rare w is negligible. Let P be a k-set with no rare w. Let $1 \le i_1 < \ldots < i_l \le L$. The root w_0 will spawn a child w_1 at the i_1-st N of w_0. Then w_1 will spawn a child w_2 at the i_2-st N of w_1. This will continue until reaching a k-th level w_k. Different $\{i_1,\ldots,i_k\}$ give different w_k so that

$$|P| \ge \binom{L}{k} = \frac{q^k}{2^k k!}\left(1 - O(q^{-1/2}\sqrt{\ln q})\right) \tag{55}$$

and the total number of k-sets in the packing is at most

$$o(2^q q^{-k-1/2}) + \frac{2^q}{\frac{q^k}{2^k k!}(1 - O(q^{-1/2}\sqrt{\ln q}))}. \tag{56}$$

which yields (54). □

Let $w = w_1 \cdots w_q$. For convenience define, for $1 \le i \le q$, $X_w(i) = +1$ if $w_i = N$ and $X_w(i) = -1$ if $w_i = Y$. Define $D_w(i)$ for $0 \le i \le q$ by setting $D_w(0) = 0$ and setting $D_w(i) = D_w(i-1) + X_w(i)$. We shall refer to D_w as the walk given by w. Set $T = 100 \ln\ln q$. (In this section we shall omit all ceilings and floors, which have no asymptotic effect.) For $0 \le t < T$ set $x_t = q(1 - 2^{-t})$. Set $x_T = q$. The x_t's split $\{1,\ldots,q\}$ into intervals, we shall refer to $(x_{t-1}, x_t]$ as the t-th interval. For $1 \le t \le T$ set $l_t = x_t - x_{t-1}$ and $\Delta_w(t) = D_w(x_{t-1}) - D_w(x_t)$. Thus l_t represents the length of the t-th interval and $\Delta_w(t)$ represents how much the walk drops in the t-th interval. Note that the argument for (54) essentially split off those w with $D_w(q) < -K\sqrt{q \ln q}$.

Let $1 \le L$ and $1 \le t < T$ be integral. We say w has a (t, L)-drop if

$$Lt\sqrt{l_t} \le \Delta_w(t) < (L+1)t\sqrt{l_t}. \tag{57}$$

We don't define (T, L)-drops. In the following proof the last interval l_T will be treated separately from l_t for $1 \le t < T$.

Fix positive c with $\frac{c^2}{2} > k + \frac{1}{2}$. Call w *rare* if $\Delta_w(t) > \sqrt{l_t}(c\sqrt{\ln q})$ for some $t \le T$. Call P rare if it contains any rare w. Basic large deviation results (see, e.g., [1]) give that a random w has $\Delta_w(t) > \beta\sqrt{l_t}$ with probability less than $\exp[-\beta^2/2]$. Thus the number of rare w is $o(2^q q^{-k-\frac{1}{2}})$ and so the number of rare P in a packing is also $o(2^q q^{-k-\frac{1}{2}})$. This is negligible for our purposes. Thus we need only show that the number of non-rare P in a packing is bounded from above by

$$\frac{2^{q+k}}{\binom{q}{k}} + c_2 2^q q^{-k-\frac{1}{2}}. \tag{58}$$

We say that $w \in P$ has *lastlie* t if the final lie position, i.e., $\max(S(w))$, lies in the t-th interval. When w is the root we say it has lastlie 0. For $1 \le t < T$ We say that $w \in P$ has a (t, L, i)-drop if

1. w has a (t, L)-drop.
2. $w \in P$ is on level i.
3. $w \in P$ has lastlie $l \le t$.

`Comments:` We can now give a non-rigorous description of what we feel is the heart of the argument. Call P super-normal if no $w \in P$ has any (t, L, i)-drop. Then all $w \in P$ would have at least $\frac{1}{2}(q - \sum_{t<T} t\sqrt{l_t} - c\sqrt{\ln q}\sqrt{l_T})$ coordinates $w_i = N$. The convergence of $\sum t2^{-t/2}$ and the choice of T so that $\sqrt{\ln q}2^{-T/2} = o(1)$ makes the number of N of the form $\frac{1}{2}(q - O(\sqrt{q}))$. Then, similar to (55), we could bound $|P| \ge \binom{q/2}{k}(1 - O(q^{-1/2}))$. If all P were super-normal then the number of P in the packing would be as desired by the simple volume bound. When $w \in P$ has a (t, L, i)-drop it will lower the value (or, at least, our lower bound on the value) of $|P|$ by an amount we shall quantify. The larger L is the more $|P|$ is decreased, but also the rarer the (t, L, i) can be. For each t, L, i we shall bound the total negative effect on the $|P|$ that (t, L, i)-drops can make. At the end the sum of these effects over all (t, L, i) is bounded essentially by a constant times the first term. The example $t = 1, L = 1, i = 0$ - P whose roots drop by between one and two standard deviations in the first interval - would be an instructive one in what follows. We also comment on requiring the t-th interval to drop by t standard deviations to be not super-normal. This factor of t has wide latitude, we could replace it by slower growing or faster growing functions of t – e.g., $(1.1)^t$ – and still have a valid argument.

We will need two technical lemmas.

Lemma 4.2. *Fix t, L and $i < k$. The total number of w in a packing of non-rare k-sets that can have a (t, L, i)-drop is bounded above by $2^q q^{i-k} e^{-L^2t^2/2} 2^{t(k-i)}(k-i)!3^{k-i}$.*

Proof. For $t < T$ a non-rare w has more than $q2^{-t}/3$ N's at positions $u > x_t$. (Indeed, non-rare w have at least roughly half of their coordinates N in every interval.) Let P be an non-rare k-set, and let $w \in P$ be on level i with the lastlie $l \le t$. A descendant of w on level k is given by a sequence $w = w_i, \ldots, w_k$. For any $1 \le t_{i+1} < \ldots < t_k \le q2^{-t}/3$ we consider the sequence in which w_j is spawned on the t_j-th N of w_{j-1} that lies after x_t. These give distinct w_k so the number of such w_k is at least $\binom{q2^{-t}/3}{k-i}$.

Consider a packing of non-rare k-sets. By the basic large deviation results the number of $w' \in \{Y, N\}^q$ with a (t, L) drop is less than $2^q e^{-L^2t^2/2}$. Let $w \in P$ have a (t, L, i) drop. We have at least $\binom{q2^{-t}/3}{k-i}$ descendant w' that differ only in positions $u > x_t$. Hence they all have a (t, L) drop. Hence the number of such w in the packing is at most

$$\frac{2^q e^{-L^2t^2/2}}{\binom{q2^{-t}/3}{k-i}} \le 2^q q^{i-k} e^{-L^2t^2/2} 2^{t(k-i)}(k-i)!3^{k-i}. \tag{59}$$

$\square$

Set

$$\Omega = \{(t,j) : 1 \le t < T, 1 \le j \le \frac{l_t - t\sqrt{l_t}}{2}\} \cup \{(T,j) : 1 \le j \le \frac{l_T - c\sqrt{\ln q}\sqrt{l_T}}{2}\} \tag{60}$$

with c satisfying $c^2/2 > k + \frac{1}{2}$ as before. Note that

$$|\Omega| = \frac{q}{2} - \sum_{t=1}^{T-1} \frac{1}{2} t\sqrt{l_t} - \frac{1}{2} c\sqrt{\ln q}\sqrt{l_T}. \tag{61}$$

We selected T sufficiently large that $\sqrt{q2^{-T}}\sqrt{\ln q} = o(q^{1/2})$. As $l_t \sim 2^{-t}q$ for $t < T$ and $\sum_{t=1}^{\infty} t\sqrt{2^{-t}}$ converges we have

$$|\Omega| = \frac{q}{2} - (c + o(1))q^{1/2} \tag{62}$$

for an absolute constant c. We shall order Ω by setting $(t,j) \le (t',j')$ if $t < t'$ or $t = t'$ and $j < j'$. For $w \in P$ the (t,j) position is that index u such that w_u is the j-th N in the t-th interval, if it exists. With w non-rare if the (t,j) position does not exist then w has a (t,L) drop for some L. (With w non-rare the (T,j) position must exist for all $(T,j) \in \Omega$.) We define Ω^* to be the set of ordered k-tuples $(t_0,j_0) < \ldots < (t_{k-1},j_{k-1})$. Then

$$|\Omega^*| = \binom{|\Omega|}{k} = \binom{q/2}{k}\left(1 - (c' + o(1))q^{-1/2}\right) \tag{63}$$

for an absolute constant c'. Fix an non-rare k-set P. For $\alpha \in \Omega^*$ of the above form we associate (when it exists) a $w_k \in P$ as follows: Let w_0 be the root of P and, for $0 \le i < k$ let w_{i+1} be spawned from w_i at the (t_i,j_i) position of w_i.

Let $\Omega^*(P)$ denote the set of $\alpha \in \Omega^*$ for which the associated w_k exists. When w_k exists it is uniquely determined. Thus

$$|P| \ge |\Omega^*(P)| = |\Omega^*| - |\Omega^* - \Omega^*(P)|. \tag{64}$$

(P also will have elements at levels $i < k$ but we shall ignore these in giving our lower bound.) For a given packing of k-sets we set

$$\Gamma = \sum_P |\Omega^* - \Omega^*(P)|, \tag{65}$$

where the sum ranges over all non-rare P in a packing. Γ is our quantitative measure of how far the non-rare P stray from supernormality. Our goal is to bound Γ from above.

Lemma 4.3.

$$\Gamma = O(2^q q^{-1/2}). \tag{66}$$

Proof. Suppose $\alpha = ((t_0,j_0),\ldots,(t_{k-1},j_{k-1})) \in \Omega^* - \Omega^*(P)$, so that the construction of the sequence $w_0,\ldots,w_k$ fails. There will be a $0 \le i < k$ such that w_i exists but does not have a (t_i,j_i) position. This w_i must have a (t_i,L,i)-drop for some L. (Note that for $i \ne 0$

w_i has lastlie $t_{i-1} \le t_i$ by the ordering.) Set $w = w_i$ and $t = t_i$ for convenience. When this occurs we say w destroys α at interval t.

Conversely, suppose $w \in P$ has a (t, L, i)-drop. It will destroy many $\alpha' \in \Omega^*$ at interval t. Such α' all begin with $(t_0, j_0), \ldots, (t_{i-1}, j_{i-1})$ to reach w. The next position must be of the form (t, j) since t is fixed. (In general, a given w may have several (t, L, i)-drops, each is considered separately.) There are at most $\frac{1}{2}Lt\sqrt{l_t}$ possibilities for j since w does not drop more than $(L+1)t\sqrt{l_t}$ in the t-th interval. There are less than $q2^{1-t}$ elements of Ω that are greater than (t, j) and so at most $\binom{q2^{1-t}}{k-1-i}$ possible extensions to an element of Ω^*. Thus the number of $\alpha' \in \Omega^*$ at interval t destroyed by w is at most

$$\frac{1}{2}q^{k-i-\frac{1}{2}}Lt2^{-t/2}(2^{1-t})^{k-1-i}/(k-1-i)!. \tag{67}$$

Any $\alpha' \in \Omega^* - \Omega^*(P)$ must be destroyed by some w at interval t. This w must have a (t, L, i)-drop for some L. For a given (t, L, i) the number of such w is bounded by (59) and the number of α' destroyed by w at interval t is bounded by (67). Thus

$$\Gamma \le \sum_{t,L,i} 2^{q-1}q^{i-k}e^{-L^2t^2/2}2^{t(k-i)}(k-i)!3^{k-i}q^{k-i-\frac{1}{2}}Lt2^{-t/2}(2^{1-t})^{k-1-i}/(k-1-i)!. \tag{68}$$

As k is bounded (and so $i < k$ is bounded),

$$\Gamma = 2^q q^{-1/2} O(\sum_{t,L,i} Lt2^{t/2}e^{-L^2t^2/2}). \tag{69}$$

The exponential decay dominates this sum for L or t large so that the sum over all integers $t \ge 0$, $L \ge 1$, $i < k$ converges. (This convergence may be regarded as the heart of the argument - while some P may be far from super-normal and thus considerably smaller their exponentially small proportion makes them a negligible effect.) This gives the critical bound:

$$\Gamma = O(2^q q^{-1/2}). \tag{70}$$

□

Now we are ready to finish the proof. Assume that a packing consists of A non-rare k-sets P. Then

$$2^q \ge \sum |P| \ge A|\Omega^*| - O(2^q q^{-1/2}). \tag{71}$$

So that, applying bound (63)

$$A \le \frac{2^q(1 + O(q^{-1/2})}{\binom{q/2}{k}(1 - O(q^{-1/2}))}. \tag{72}$$

Adding in the rare P and letting $A = A_k(q)$ be the maximal value,

$$A_k(q) \le \frac{2^q}{\binom{q/2}{k}}(1 + O(q^{-1/2})) + o(2^q q^{-k-\frac{1}{2}}). \tag{73}$$

which complete the upper bound of Theorem 1.1.

References

[1] N. Alon and J. Spencer, The Probabilistic Method, 2nd ed., John Wiley, 2000.

[2] E.R. Berlekamp, Block coding for the binary symmetric channel with noiseless, delayless feedback, In *Error-correcting codes*, H.B. Mann (ed.), Wiley (1968), 61-88

[3] F. Cicalese and D. Mundici, Optimal coding with one asymmetric error: below the Sphere Packing bound, In *Proceedings of 6th Annual International Conference on Computing and Combinatorics*–COCOON'2000, *Lecture Notes in Computer Science*, **1858**, pp. 159–169, Springer–Verlag, 2000.

[4] I. Dumitriu and J. Spencer, A Halfliar's Game, *Theoretical Computer Science*, Ser. A. (to appear)

[5] A. Pelc, Solution to Ulam's problem on searching with a lie, *J. Combinatorial Theory*, Ser. A. **44** (1987), 129-142

[6] A. Pelc, Searching games with errors – fifty years of coping with liars, *Theoretical Computer Science* **270** (2002), 71–109

[7] A. Rényi, *A Diary on Information Theory*, J. Wiley and Sons (1984), (original publication: *Napló az információelméletről*, Gondolat, Budapest, 1976).

[8] J. Spencer, Ulam's searching problem with a fixed number of lies, *Theoretical Computer Science* **95** (1992), 307-321

[9] R. P. Stanley. Enumerative Combinatorics, Vol. 2. Cambridge University Press, 1999.

[10] S. M. Ulam, *Adventures of a Mathematician*, Scribners, 1976.