Inverse Littlewood-Offord theory

Van H. Vu

Department of Mathematics
Rutgers University

Let $\mathbf{v} = \{a_1, \ldots, a_n\}$ be a set of n non-zero numbers and $\xi_1, \ldots, \xi_n$ be i.i.d random Bernoulli variables. Define

$$S := \sum_{i=1}^{n} \xi_i a_i.$$

Discrete. Define $p_{\mathbf{v}}(a) := \mathbf{P}(S = a)$ and

$$p_{\mathbf{v}} := \sup_{a \in \mathbf{Z}} p_{\mathbf{v}}(a).$$

Continuous. Define $p_{\mathbf{v},\beta}(a) := \mathbf{P}(|S - a| \leq \beta)$ and

$$p(\mathbf{v}, \beta) := \sup_{a \in \mathbf{R}} p_{\mathbf{v},\beta}(a).$$

In their study of random polynomials, Littlewood and Offord (1940s) raised the question of bounding $p(\mathbf{v})$ and $p(\mathbf{v}, \beta)$. They showed

$$p_{\mathbf{v}} = O(\frac{\log n}{\sqrt{n}}).$$

Very soon after, Erdős, using Sperner's lemma, proved

Theorem (Littlewood-Offord-Erdős)

Let $a_1, \ldots, a_n$ be non-zero numbers and ξ_i be i.i.d Bernoulli random variables. Then

$$p_{\mathbf{v}} \leq \frac{\binom{n}{\lfloor n/2 \rfloor}}{2^n} = O(\frac{1}{\sqrt{n}}).$$

Notice that the bound is sharp, as can be seen from the example $\mathbf{v} := \{1, \ldots, 1\}$, in which case S has a binomial distribution.
By Freiman's isomorphism, in the discrete version we can assume that the a_i are integers.

Theorem LOE is a classical result in combinatorics and has generated lots of research, in particular from the 1960s to late 1980s. It has been realized that while the bound is sharp, it can be improved significantly under additional assumptions on $\mathbf{v}$.

- Erdős and Moser (1960s) showed that if the a_i are distinct, then

$$p_{\mathbf{v}} = O(n^{-3/2} \ln n).$$

- They conjectured that the logarithmic term is not necessary and this was confirmed by Sárközy and Szemerédi (1960s) . Again, the bound is sharp (up to a constant factor), as can be seen by taking $a_1, \ldots, a_n$ to be a proper arithmetic progression such as $1, \ldots, n$.
- Stanley gave a different proof (based on the hard Lefchetz theorem in algebraic geometry) that also classified the extremal cases, which turns out to be Arithmetic progressions (any algebraic proof was given later by Proctor).

Halász obtained a general theorem, which, among others, showing that if one forbids more and more additive structure in the a_i, then one gets better and better bounds on $p_{\mathbf{v}}$.

Theorem (Halász 1970s)

Consider $\mathbf{v} = \{a_1, \ldots, a_n\}$. *Let* R_k *be the number of solutions to the equation*

$$\epsilon_1 a_{i_1} + \cdots + \epsilon_{2k} a_{i_{2k}} = 0$$

where $\epsilon_i \in \{-1, 1\}$ *and* $i_1, \ldots, i_{2k} \in \{1, 2, \ldots, n\}$. *Then*

$$p_{\mathbf{v}} = O_k(n^{-2k-1/2} R_k).$$

Many related results: Katona, Kleitman, Griggs-Lagarias-Odlyzko-Shearer, Füredi-Frankl, Sali, Beck, Wooley et. al etc.

Inverse Theory. (Tao-V. 05) Instead of trying to improve the bound further by imposing new assumptions, we aim to find the underlying reason for the probability $p_{\mathbf{v}}$ to be large (say, polynomial in n).

Inverse Theory. (Tao-V. 05) Instead of trying to improve the bound further by imposing new assumptions, we aim to find the underlying reason for the probability $p_{\mathbf{v}}$ to be large (say, polynomial in n).

Intuition. The (multi)-set $\mathbf{v}$ has 2^n subsums, and $p_{\mathbf{v}} \geq n^{-C}$ mean that at least $2^n/n^C$ among these take the same value. This suggests that the set has strong additive structure.

In order to determine this structure, we first study examples of $\mathbf{v}$ where $p_{\mathbf{v}}$ is large. For a set A, we denote by lA the set

$$lA := \{a_1 + \cdots + a_l | a_i \in A\}.$$

Example 1. Let $I = [-N, N]$ and $a_1, \ldots, a_n$ be elements of I. Since $S \in nI$, by the pigeon hole principle, $p_{\mathbf{v}} \geq \frac{1}{n|I|} = \Omega(\frac{1}{nN})$.

Example 1. Let $I = [-N, N]$ and $a_1, \ldots, a_n$ be elements of I. Since $S \in nI$, by the pigeon hole principle, $p_{\mathbf{v}} \geq \frac{1}{n|I|} = \Omega(\frac{1}{nN})$.

In fact, a short consideration yields a better bound. Notice that with probability at least .99, we have $S \in 10\sqrt{n}I$, thus again by the pigeonhole principle, we have $p_{\mathbf{v}} = \Omega(\frac{1}{\sqrt{n}N})$. If we set $N = n^C$ for some constant C, then

$$p_{\mathbf{v}} = \Omega(\frac{1}{n^{C+1/2}}). \tag{1}$$

The next, and more general, construction comes from *additive combinatorics*.
A set Q of numbers is a *GAP of rank d* (Generalized Arithmetic Progression) if it can be expressed as in the form

$$Q = \{a_0 + x_1 a_1 + \cdots + x_d a_d | 0 \leq x_i \leq M_i \text{ for all } 1 \leq i \leq d\}$$

for some $a_0, \ldots, a_d, M_1, \ldots, M_d$.
It is convenient to think of Q as the image of an integer box $B := \{(x_1, \ldots, x_d) \in \mathbf{Z}^d | 0 \leq m_i \leq M_i\}$ under the linear map

$$\Phi : (x_1, \ldots, x_d) \mapsto a_0 + x_1 a_1 + \cdots + x_d a_d.$$

The numbers a_i are the *generators* of P, and $\mathbf{Vol}(Q) := |B|$ is the *volume* of B. We say that Q is *proper* if this map is one to one, or equivalently if $|Q| = \mathbf{Vol}(Q)$. For non-proper GAPs, we of course have $|Q| < \mathbf{Vol}(Q)$.

Example 2. Let Q be a proper GAP of rank d and volume V. Let $a_1, \ldots, a_n$ be (not necessarily distinct) elements of P. The random variable $S = \sum_{i=1}^{n} \xi_i a_i$ takes values in the GAP nP. Since $|nP| \leq \mathbf{Vol}(nB) = n^d V$, the pigeonhole principle implies that $p_{\mathbf{v}} \geq \Omega(\frac{1}{n^d V})$.

Example 2. Let Q be a proper GAP of rank d and volume V. Let $a_1, \ldots, a_n$ be (not necessarily distinct) elements of P. The random variable $S = \sum_{i=1}^{n} \xi_i a_i$ takes values in the GAP nP. Since $|nP| \leq \mathbf{Vol}(nB) = n^d V$, the pigeonhole principle implies that $p_{\mathbf{v}} \geq \Omega(\frac{1}{n^d V})$.

Using the same idea as in the previous example, one can improve the bound to $\Omega(\frac{1}{n^{d/2} V})$. If we set $N = n^C$ for some constant C, then

$$p_{\mathbf{v}} = \Omega(\frac{1}{n^{C+d/2}}). \tag{2}$$

The above examples show that if the elements of $\mathbf{v}$ belong to a proper GAP with small rank and small cardinality then $p_{\mathbf{v}}$ is large.

The above examples show that if the elements of $\mathbf{v}$ belong to a proper GAP with small rank and small cardinality then $p_{\mathbf{v}}$ is large.

The above examples show that if the elements of $\mathbf{v}$ belong to a proper GAP with small rank and small cardinality then $p_{\mathbf{v}}$ is large.

This turns out to be (essentially) the only reason !

The above examples show that if the elements of $\mathbf{v}$ belong to a proper GAP with small rank and small cardinality then $p_{\mathbf{v}}$ is large.

This turns out to be (essentially) the only reason !

Theorem (Weak inverse theorem, Tao-V. 06)

Let $C, 1 > \epsilon > 0$ be arbitrary constants. There are constants d and C' depending on C and ϵ such that the following holds. Assume that $\mathbf{v} = \{a_1, \ldots, a_n\}$ is a multiset of integers satisfying $p_{\mathbf{v}} \geq n^{-C}$. Then there is a GAP Q of rank at most d and volume at most $n^{C'}$ which contains all but at most $n^{1-\epsilon}$ elements of $\mathbf{v}$ (counting multiplicities).

The presence of the small set of exceptional elements is not completely avoidable.

The presence of the small set of exceptional elements is not completely avoidable.

We call the above theorem *weak inverse* as the dependence between the parameters is not optimal and does not yet reflect the relations in (1) and (2).

Theorem (Strong inverse theorem, Tao-V. 08)

Let C and $1 > \epsilon$ be positive constants. Assume that

$$p_{\mathbf{v}} \geq n^{-C}.$$

Then there exists a GAP Q of rank $d = O_{C,\epsilon}(1)$ which contains all but $O_d(n^{1-\epsilon})$ elements of $\mathbf{v}$ (counting multiplicity), where

$$|Q| = O_{C,\epsilon}(n^{C-\frac{d}{2}+\epsilon}).$$

Main tools. Fourier analysis, theory of random walks and a replacement principle.

The ϵ error term seems to be the limit of the method.

The Optimal Inverse Theorem.

Using a different approach

Theorem (Optimal inverse theorem, Nguyen-V. 09)

Let C and $1 > \epsilon$ be positive constants. Assume that

$$\rho := p_{\mathbf{v}} \geq n^{-C}.$$

Then there exists a GAP Q of rank $d = O_{C,\epsilon}(1)$ which contains all but ϵn elements of $\mathbf{v}$ (counting multiplicity), where

$$|Q| = O(\rho^{-1} n^{-d/2}) = O(n^{C - \frac{d}{2}}).$$

Main tools. Fourier analysis, Halász level set argument, long range Freiman theorem.

Continuous version

The continuos version asserts that the numbers a_i lie close to the points of a GAP with small dimension and volume.

Theorem (Optimal inverse Littlewood-Offord theorem, continuous case, Nguyen-V. 09)

Let $\delta, C, C' > 0$ be arbitrary constants and $\beta \geq n^{-C'}$ be a parameter that may depend on n. Suppose that $\mathbf{v} = \{a_1, \dots, a_n\}$ are vectors in R^d of norm at least one and

$$p(\mathbf{v}, 1) \geq n^{-C}.$$

Then there exists a proper symmetric GAP Q of rank $r = O(1)$ which is $O(\frac{\log n}{n^{1/2}})$-close to all but at most δn elements of $\mathbf{v}$ (counting multiplicity), where

$$|Q| = O(\rho^{-1} n^{(-r+d)/2}).$$

Related works

One can also have inverse theorems under a different assumption or weaker assumption.

Tao-Vu (2005): Similar characterization, under a different assumption.

Rudelson-Vershynin (07): Different characterization involving only AP (not GAP), but allow $\rho := p(\mathbf{v})$ to be exponentially small in n; require some extra conditions such as the a_i are comparable in order of magnitude.

Long range Freiman theorem

Theorem (Freiman's inverse theorem)

Let γ be a positive constant and X a subset of a torsion-free group such that $|2X| \leq \gamma|X|$. Then there is a proper symmetric GAP Q of rank at most $r = O_\gamma(1)$ and cardinality $O_\gamma(|X|)$ such that $X \subset Q$.

In our analysis, we will need to deal with an assumption of the form $|kX| \leq k^\gamma|X|$, where γ is a constant, but k is not. (Typically, k will be a positive power of $|X|$.)

Theorem (Long range Freiman theorem)

Let $\gamma > 0$ be constant. Assume that X is a subset of a torsion-free group such that $0 \in X$ and $|kX| \leq k^\gamma|X|$ for some positive integer $k \geq 2$. Then there is proper symmetric GAP Q of rank $r = O(\gamma)$ and cardinality $O_\gamma(k^{-r}|kX|)$ such that $X \subset Q$.

Tools. Szmerédi-V. iteration argument.

Proof of optimal theorem

- Embed the problem into F_p for some large prime p.
- By the assumption

$$\rho := n^{-C} \leq \frac{1}{p} \sum_{\xi \in F_p} \prod_{i=1}^{n} |\cos 2\pi a_i \xi / p| \leq \frac{1}{p} \sum_{\xi \in F_p} \exp(-\sum_{i=1}^{n} c \|a_i \xi\|^2),$$

  where $\|x\|$ is the distance from x/p to 0.
- Level set $S_m := \{\xi | \sum_{i=1}^{n} c\|a_i \xi\|^2 \leq m\}$. There is a large level set S_m such that

$$|S_m| \exp(-m/2) \geq \rho p$$

  for some m.

- On the other hand $\sum_{i=1}^{n} \sum_{\xi \in S_m} \|a_i \xi\|^2 \leq m|S_m|$ by definition. So, for most a_i

$$\sum_{\xi \in S_m} \|a_i \xi\|^2 \leq \frac{C_0 m}{n} |S_m|$$

for some large constant C_0.

- Assume that all $a_i \in \mathbf{v}$ have this property. By Cauchy-Schwartz, for any $a \in k\mathbf{v}$

$$\sum_{\xi \in S_m} \|a\xi\|^2 \leq k^2 \frac{C_0 m}{n} S_m.$$

- On the other hand, let $\mathbf{v}^* := \{a | \sum_{\xi \in S_m} \|a\xi\|^2 \leq c_0 |S_m|\}$ for some small c_0. Then one can show

$$|\mathbf{v}^*| = O(p/|S_m|).$$

  (One can consider the toy case $S_m = \{1, \ldots, L\}$.)
- Set $k = c_1 \sqrt{n/m}$, for a properly chosen c_1, we have $k\mathbf{v} \subset \mathbf{v}^*$, so $|k\mathbf{v}|$ is *small.*
- Use *long range* Freiman theorem.

Applications

Application 1 Reprove many asymptotic *forward* results.

Applications

Application 1 Reprove many asymptotic *forward* results.

For instance, let us reprove Sárközy-Szemerédi theorem that if the a_i are different, then $\rho := p_{\mathbf{V}} \leq Kn^{-3/2}$ (for some constant $K > 0$).

Applications

Application 1 Reprove many asymptotic *forward* results.

For instance, let us reprove Sárközy-Szemerédi theorem that if the a_i are different, then $\rho := p_{\mathbf{v}} \leq Kn^{-3/2}$ (for some constant $K > 0$).

The Optimal Inverse Theorem implies that most of $\mathbf{v}$ is contained in a GAP Q of rank d and cardinality at most

$$O(\rho^{-1}n^{-d/2}) = O(\rho^{-1}n^{-1/2}) = O(K^{-1}n).$$

Set K be sufficiently large constant, the RHS is less than $\frac{1}{2}n$, a contradiction.

Applications

Applications 2. Random matrix theory

- Singularity bound for random Bernoulli matrices (Tao-V. 05, Bourgain-V. -Wood 09).
- Least singular value (Tao-V. 06, Rudelson-Vershynin 07).
- Circular law (β-net lemma) (Tao-V. 08).
- Multiplicities of eigenvalues (Tao-V. 10).

Applications

Application 3. Precise results.

Use the structure theorem as a base to obtain sharp result.

Stanley revisited

Stanley result shows that in the case the a_i are different, the extremal set is an arithmetic progression.
Argument: There is an operator T that transforms a set $\mathbf{v}$ in a *better* set $\mathbf{v}'$. The fixed point is an arithmetic progression.

Stanley revisited

Stanley result shows that in the case the a_i are different, the extremal set is an arithmetic progression.
Argument: There is an operator T that transforms a set $\mathbf{v}$ in a *better* set $\mathbf{v}'$. The fixed point is an arithmetic progression.

This does not give numerics bound: $(C + o(1))n^{-3/2}$. What is C ?

Stanley revisited

Stanley result shows that in the case the a_i are different, the extremal set is an arithmetic progression.
Argument: There is an operator T that transforms a set $\mathbf{v}$ in a *better* set $\mathbf{v}'$. The fixed point is an arithmetic progression.

This does not give numerics bound: $(C + o(1))n^{-3/2}$. What is C ?

Equivalent problem: How many subsets of $\{-n/2, ..., n/2\}$ sums up to zero ?

Lemma (Asymptotic bound, Nguyen 09)

$$C = \sqrt{24/\pi}.$$

Lemma (Asymptotic bound, Nguyen 09)

$$C = \sqrt{24/\pi}.$$

Theorem (Stability Theorem, Nguyen 09)

Let $\epsilon > 0$ be a sufficiently small constant. Assume that V is a set of size n such that $p_{\mathbf{v}} \geq (1-\epsilon)Cn^{-3/2}$. Then there exists k such that $\mathbf{v} = k \cdot \mathbf{v}'$ and $\sum_{w \in \mathbf{v}'} |w|^2 \leq (1+\epsilon')n^3/12$, where ϵ' tends to zero with ϵ.

The proof, in a sense, shows that to make $p(\mathbf{v})$ large, one would need the variance $a_1^2 + \cdots + a_n^2$ to be small. The minimum is obtained by $\{-\lfloor n/2 \rfloor, \ldots, \lfloor n/2 \rfloor\}$.

Frankl-Füredi conjecture

General question. Determine exactly the maximum probability that the random sum $S := \sum_{i=1}^{n} a_i \xi_i$ is contained in a ball of radius Δ ($p(\mathbf{v}, Delta)$).
Define $s := \lfloor \Delta \rfloor + 1$. Consider $\mathbf{v} := \{a_1, \ldots, a_n\}$, $|a_i| \geq 1$.

Theorem (Erdős, 40s)

Let $S(n, m)$ denote the sum of the largest m binomial coefficients $\binom{n}{i}, 0 \leq i \leq n$. Then

$$p(\mathbf{v}, \Delta) = 2^{-n} S(n, s).$$

The situation for higher dimension is more complicated. Frankl and Füredi (88) sharpening several results proved

Theorem (Frankl-Füredi)

Consider $\mathbf{v} := \{a_1, \ldots, a_n\}$, $a_i \in R^2, \|a_i\| \geq 1$.

$$p(\mathbf{v}, \Delta) = (1 + o(1))2^{-n} S(n, s)$$

Question. Can one have the exact estimate $p(\mathbf{v}, \Delta) = 2^{-n} S(n, s)$?

In general this is not true. It was observed (Kleiman, FF) that the exact estimate fails if $s \geq 2$ and

$$\Delta > \sqrt{(s-1)^2 + 1}.$$

Example. Take $v_1 = \cdots = v_{n-1} = e_1$ and $v_n = e_2$, where e_1, e_2 are two orthogonal unit vectors. For this system, there is a ball B of radius Δ such that $\mathbf{P}(S \in B) > S(n, s)$.

Conjecture Let Δ, d be fixed. If $s - 1 \leq \Delta < \sqrt{(s-1)^2 + 1}$ and n is sufficiently large, then $p(n, \Delta) = 2^{-n} S(n, s)$.

Confirmed: $s = 1$ (Kleitman); $s = 2, 3$ (Frankl and Füredi).
Frankl and Füredi also showed that the precise bound holds under a stronger assumption that $s - 1 \leq \Delta \leq (s-1) + \frac{1}{10s^2}$.

Proof of FF conjecture

Tao-V. (10) confirm the conjecture for $s > 3$, using the following inverse theorem

Theorem

Assume $a_i \in R^d$ having norm at least one. If $p(\mathbf{v}, 1) \geq Ck^{-d/2}$, then all but k elements of $\mathbf{v}$ has distance less than one to a hyperplane. ($C = C(d)$ is a sufficiently chosen constant.)

Let's first reprove FF asymptotic theorem, using induction on d. The case $d = 1$ was done by Erdős. Assume that $d \geq 2$; need to show

$$p(n, \Delta) \leq (1 + \epsilon)2^{-n} S(n, s).$$

Suppose the claim failed, then there exists $\Delta > 0$ such that for arbitrarily large n, there exist a family $\mathbf{v} = \{a_1, \ldots, a_n\}$ of vectors in R^d of length at least 1 and a ball B of radius Δ such that (with $S := \sum_{i=1}^{n} a_i \xi_i$)

$$\mathbf{P}(S \in B) \geq (1 + \epsilon)2^{-n} S(n, s) = \Omega(n^{-1/2}).$$

By the pigeonhole principle, there is a ball B_1 of radius $\frac{1}{\log n}$

$$\mathbf{P}(S \in B_1) = \Omega(n^{-1/2} \log^{-d} n) \geq C k^{-d/2},$$

with $k := n^{2/3}$, as $d \geq 2$.

Applying Inverse theorem in the contrapositive (rescaling by $\log n$), find a hyperplane H such that $dist(a_i, H) \leq 1/\log n$ for at least $n - k$ values of $i = 1, \ldots, n$.

Let $\mathbf{v}'$ be the orthogonal projection to H of a_i with $dist(v_i, H) \leq 1/\log n$. By conditioning on the signs of all the ξ_i with $dist(v_i, H) > 1/\log n$, and then projecting the sum S onto H, we conclude that there is a $d-1$-dimensional ball B' in H of radius Δ such that

$$\mathbf{P}(S' \in B') \geq (1+\epsilon)2^{-n} S(n,s) \geq (1+\epsilon/2)2^{-n'} S(n',s).$$

Notice the vectors in $\mathbf{v}'$ have magnitude at least $1 - 1/\log n$. Rescaling the $\mathbf{v}'$ by $(1 - 1/\log n)^{-1}$ (which *does not* change s), one obtains a contradiction on $d-1$ dimension.

Now we consider the conjecture. Assume $s \geq 3$. If the conjecture failed, then there exist a family $\mathbf{v} = \{a_1, \ldots, a_n\}$ of vectors in $\mathbf{R}^d$ of length at least 1 and a ball B of radius Δ

$$\mathbf{P}(X_V \in B) > 2^{-n} S(n, s).$$

By iterating the previous argument, we may find a one-dimensional subspace L of $\mathbf{R}^d$ such that $dist(v_i, L) \leq 1/\log n$ for $i = 1, \ldots, n-k, k = O(n^{2/3}$. Let $\pi : \mathbf{R}^d \to L$ be the orthogonal projection map.

Case 1. $|\pi(v_i)| > \frac{\Delta}{s}$ for all $1 \leq i \leq n$. Use the trivial bound

$$\mathbf{P}(S(\mathbf{v}) \in B) \leq \mathbf{P}(S(\pi(\mathbf{v})) \in \pi(B)).$$

Rescale Erdős' theorem by a factor slightly less than s/Δ (notice that $\lfloor \Delta(\frac{s}{\Delta} - \epsilon) \rfloor = s - 1$ for any $\epsilon > 0$), we have

$$\mathbf{P}(S(\pi(\mathbf{v})) \in \pi(B)) \leq 2^{-n} S(n, s),$$

a contradiction.

Case 2. $|\pi(v_n)| \leq \Delta/s$. We let $\mathbf{v}'$ be the vectors $a_1, \ldots, a_{n-k}$. By conditioning on the $\xi_{n-k+1}, \ldots, \xi_{n-1}$, there is a ball B' of radius Δ such that

$$\mathbf{P}(S(\mathbf{v}') + \xi_n v_n \in B') \geq \mathbf{P}(S(\mathbf{v}) \in B).$$

Let $x_{B'}$ be the center of B'. Observe that if $S(\mathbf{v}') + \xi_n v_n \in B'$ (for any value of ξ_n) then $|S(\pi(V')) - \pi(x_{B'})| \leq \Delta + \frac{\Delta}{s}$.

Furthermore, if $|S(\pi(\mathbf{v}')) - \pi(x_{B'})| > \sqrt{\Delta^2 - 1}$, then the *parallelogram law* shows that $S(\mathbf{v}') + v_n$ and $S(\mathbf{v}') - v_n$ cannot both lie in B'. Conditioned on $|S(\pi(V')) - \pi(x_{B'})| > \sqrt{\Delta^2 - 1}$

$$\mathbf{P}(S(\mathbf{v}') + \xi_n v_n \in B') \leq 1/2.$$

We conclude that

$$\mathbf{P}(X_{V'} + \xi_n v_n \in B')$$

$$\leq \mathbf{P}(|X_{\pi(V')} - \pi(x_{B'})| \leq \sqrt{\Delta^2 - 1}) + \frac{1}{2}\mathbf{P}(\sqrt{\Delta^2 - 1} < |X_{\pi(V')} - \pi(x_{B'})|$$

$$= \frac{1}{2}\Big(\mathbf{P}(|X_{\pi(V')} - \pi(x_{B'})| \leq \sqrt{\Delta^2 - 1}) + \mathbf{P}(|X_{\pi(V')} - \pi(x_{B'})| \leq \Delta + \frac{\Delta}{s}$$

By the assumption Δ satisfies

$$\sqrt{\Delta^2 - 1} < s - 1 \leq \Delta < \Delta + \frac{\Delta}{s} < s.$$

By Erdős' theorem, we conclude that

$$\mathbf{P}(|X_{\pi(V')} - \pi(x_{B'})| \leq \sqrt{\Delta^2 - 1}) \leq 2^{-(n-k)} S(n-k, s-1)$$

$$\mathbf{P}(|\pi(X_{V'}) - \pi(x_{B'})| \leq \Delta + \frac{\Delta}{s}) \leq 2^{-(n-k)} S(n-k, s).$$

The contradiction follows by Sterling formula; the gain of $\frac{1}{2}$ is essential.

Happy Birth Day, Endre !!