On a limit theorem in combinatorical analysis

By P. ERDŐS (Budapest) and H. HANANI (Haifa)

Given a set E of n elements and given positive integers $k, l, (l \leqq k \leqq n)$, we understand by $M(k, l, n)$ a minimal system of k-tuples (subsets of E having k elements each) such that every l-tuple is contained in at least one k-tuple of the system. Similarly we denote by $m(k, l, n)$ a maximal system of k-tuples such that every l-tuple is contained in at most one set of the system. The number of k-tuples in these systems will be denoted by $\overline{\overline{M}}(k, l, n)$ and $\overline{\overline{m}}(k, l, n)$ respectively.

Further we denote

$$\mu(k, l, n) = \overline{\overline{M}}(k, l, n) \cdot \frac{\binom{k}{l}}{\binom{n}{l}}, \quad \nu(k, l, n) = \overline{\overline{m}}(k, l, n) \cdot \frac{\binom{k}{l}}{\binom{n}{l}}.$$

Trivially

$$\nu(k, l, n) \leqq 1 \leqq \mu(k, l, n) \tag{1}$$

holds. It can also be easily verified that the equalities in (1) can hold only if

$$\frac{\binom{n-h}{l-h}}{\binom{k-h}{l-h}} = \text{integer}, \qquad (h = 0, 1, \ldots, l-1), \tag{2}$$

(see e. g. [4]). So far it has been proved that under condition (2) the equalities in (1) hold for $l=2$, $k=3, 4, 5$ (see [5]) and for $l=3$, $k=4$ (see [4]). R. C. BOSE suggested that perhaps the equalities in (1) hold for $l=2$ and every k if n satisfying (2) is sufficiently large.

On the other hand it has been already conjectured by EULER [2] and proved by TARRY [9] that for $l=2$, $k=6$ and $n=36$ the equalities in (1) do not hold though the condition (2) is satisfied.

For general n the problem has been solved completely by FORT and HEDLUND [3] for the case $l=2$, $k=3$.

ERDŐS and RÉNYI [1] proved that for every k

$$\lim_{n\to\infty} \mu(k, 2, n) = \gamma_k \tag{3}$$

exists with

$$\lim_{k\to\infty} \gamma_k = 1 \tag{4}$$

and moreover that for $k=p$ and $k = p+1$ (where p is a power of a prime)

(5) $$\gamma_p = \gamma_{p+1} = 1.$$

It can be easily seen that the two statements

(6) $$\lim_{n\to\infty} \mu(k, l, n) = 1, \quad \lim_{n\to\infty} \nu(k, l, n) = 1$$

are equivalent and it may be conjectured that (6) holds for every k and l.

We shall prove that (6) holds for $l=2$ and every k and also for $l=3$ and $k=p+1$.

Theorem 1. *For every integer k $(k \geqq 2)$:*

(7) $$\lim_{n\to\infty} \mu(k, 2, n) = \lim_{n\to\infty} \nu(k, 2, n) = 1.$$

PROOF. By (6) it suffices to prove

(8) $$\lim_{n\to\infty} \nu(k, 2, n) = 1.$$

We fix the integer k and assume that

(9) $$\varliminf_{n\to\infty} \nu(k, 2, n) = 1 - \varepsilon.$$

We show that for every positive integer d

(10) $$\varliminf_{n\to\infty} \nu(k, 2, dn) = \varliminf_{n\to\infty} \nu(k, 2, n) = 1 - \varepsilon.$$

Trivially

(11) $$\varliminf_{n\to\infty} \nu(k, 2, dn) \geqq \varliminf_{n\to\infty} \nu(k, 2, n).$$

Further let $t = dn + r$, $(r < d)$ then

$$\overline{m}(k, 2, t) \geqq \overline{m}(k, 2, dn)$$

and therefore

$$\nu(k, 2, t) \geqq \nu(k, 2, dn) \cdot \frac{dn(dn-1)}{t(t-1)}.$$

Consequently

$$\varliminf_{n\to\infty} \nu(k, 2, t) \geqq \varliminf_{n\to\infty} \nu(k, 2, dn)$$

and from (11), (10) follows.

Suppose that $n = kg$ where g is a multiple of $(k!)^2$. Divide the set E having n elements into k sets E_i $(i = 1, 2, \ldots, k)$ of g elements each. It is well known [8, 5] that there exist g^2 k-tuples such that each of them has exactly one element in each E_i and any two of them have at most one element in common.

We form the system $m(k, 2, n)$ by taking the mentioned g^2 k-tuples and further by taking all the k-tuples of the systems $m(k, 2, g)$ constructed on each of the sets E_i $(i = 1, 2, \ldots, k)$.

If g is sufficiently large we have by (9), $\nu(k, 2, g) > 1 - \frac{3}{2}\varepsilon$ and thus

$$\nu(k, 2, n) > \frac{k(k-1)}{n(n-1)}\left[g^2 + k\,\frac{g(g-1)}{k(k-1)}\left(1 - \frac{3}{2}\varepsilon\right)\right] \geqq 1 - \frac{3}{2k}\,\varepsilon$$

which contradicts (10).

Theorem 2. *If p is a power of a prime then*

$$\lim_{n\to\infty} \mu(p+1, 3, n) = \lim_{n\to\infty} \nu(p+1, 3, n) = 1. \tag{12}$$

PROOF. We shall use the notion of a finite Möbius geometry introduced by HANANI [6]. If p is a power of a prime then a Möbius geometry $MG(p, r)$ is a set of $p^r + 1$ elements forming a Galois field in which circles are defined as bilinear transformations of any line of the corresponding finite Euclidean geometry $EG(p, r)$ to which the additional element ∞ has been adjoined. It is proved that any triple of elements in $MG(p, r)$ is included in exactly one circle and that every circle has $p+1$ elements. Using this construction our proof will be basically on the same lines as the proof of the theorem for $l = 2$ given by ERDŐS and RÉNYI [1] except for a simplification.

By (6) it suffices to prove

$$\lim_{n\to\infty} \nu(p+1, 3, n) = 1. \tag{13}$$

For $n = p^r + 1$, $MG(p, r)$ exists and therefore

$$\nu(p+1, 3, p^r+1) = 1. \tag{14}$$

By a simple computation it can be verified that to every $\varepsilon > 0$ there exists an η depending on ε only such that

$$\nu(p+1, 3, n) > 1 - \varepsilon, \quad (p^r + 1 \leqq n < p^r(1+\eta)). \tag{15}$$

Take all the prime-powers q_i

$$p^r = q_0 < q_1 < q_2 < \ldots < q_t \leqq p^r(1+\eta). \tag{16}$$

By the theorem of HOCHEISEL and INGHAM [7] we have for p^r sufficiently large

$$q_{i+1} - q_i < q_i^{5/8}. \tag{17}$$

For every i, $(i = 0, 1, \ldots, t)$ form the Möbius geometrices $MG(q_i, s)$ where s runs through all the integers between $(\log q_0)^2$ and $q_0^{1/4}$. We have

$$\nu(q_i + 1, 3, q_i^s + 1) = 1, \qquad (i = 0, 1, \ldots, t)$$

and by (15) and (16)

$$\nu(p+1, 3, q_i^s + 1) \geqq \nu(q_i + 1, 3, q_i^s + 1)\cdot\nu(p+1, 3, q_i + 1) > 1 - \varepsilon, \tag{18}$$

$$(i = 0, 1, \ldots, t;\ (\log q_0)^2 \leqq s \leqq q_0^{1/4}).$$

From (17) it follows that for $s < q_0^{1/4}$

$$q_i^s(1+\eta) > q_{i+1}^s \tag{19}$$

and therefore for n satisfying $q_i^s < n \leqq q_{i+1}^s$, $(i = 0, 1, \ldots, t)$ it follows from (15) and (18)

$$\nu(p+1, 3, n,) > 1 - 2\varepsilon \tag{20}$$

and consequently (20) holds for every n satisfying $q_0^s < n \leqq q_t^s$.

Considering $q_t/q_0 > 1 + \frac{1}{2}\eta$ and $s \geqq (\log q_0)^2$ it follows $(q_t/q_0)^s > q_0$ and therefore

$$q_0^{s+1} < q_t^s, \qquad ((\log q_0)^2 \leqq s \leqq q_0^{1/4}).$$

Consequently (20) holds for every n satisfying

$$q_0^{[(\log q_0)^2]+1} < n < q_t^{[q_0^{1/4}]}. \tag{21}$$

Denote by I_r the interval defined in (21). It remains to be proved that for sufficiently large r the intervals I_r overlap. This means that

$$(p^{r+1})^{[(\log p^{r-1})^2]+1} < q_t^{[q_0^{1/4}]}$$

which is evident.

Bibliography

[1] P. ERDŐS and A. RÉNYI, On some combinatorial problems, *Publ. Math. Debrecen* **4** (1956), 398–405.

[2] L. EULER, Recherches sur une nouvelle espèce de quarrés magiques. L. Euleri Opera Omnia, *Teubner*, ser. I. vol. 7 (1923), 291–392.

[3] M. K. FORT, JR. and G. A. HEDLUND, Minimal coverings of pairs by triples, *Pacific J. Math.* **8** (1958), 709–719.

[4] H. HANANI, On quadruple systems, *Canad. J. Math.* **12** (1960), 145–157.

[5] H. HANANI, The existence and construction of balanced incomplete block designs, *Ann. Math. Statist.* **32** (1961), 361–386.

[6] H. HANANI, On some tactical configurations, *Canad. J. Math.* **15** (1963), 702–722.

[7] A. INGHAM, On the difference between consecutive primes, *Quart. J. Math. Oxford Ser.* **8** (1937), 255–266.

[8] H. F. MACNEISH, Euler squares, *Ann. of Math.* **23** (1922), 221–227.

[9] G. TARRY, Le problème des 36 officiers, *C. R. Assoc. Franc. Av. Sci.* **1** (1900), 122–123 and **2** (1901), 170–203.

(Received January 25, 1962)