On The Lottery Problem

Zoltán Füredi*
Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL 61801-2917
Mathematical Institute of the Hungarian Academy of Sciences, Budapest 1364 Hungary

Gábor J. Székely†
Department of Mathematics, Technical University, 1521 Budapest, Hungary
Department of Mathematics and Statistics, Bowling Green State University, Bowling Green, OH 43403-0221

Zoltán Zubor
Department of Mathematics, Technical University, 1521 Budapest, Hungary

ABSTRACT

Let $L(n,k,k,t)$ denote the minimum number of k-subsets of an n-set such that all the $\binom{n}{k}$ k-sets are intersected by one of them in at least t elements. In this article $L(n,k,k,2)$ is calculated for infinite sets of n's. We obtain $L(90,5,5,2) = 100$, i.e., 100 tickets needed to guarantee 2 correct matches in the Hungarian Lottery. The main tool of proofs is a version of Turán's theorem due to Erdős. © 1996 John Wiley & Sons, Inc.

1. STEINER SYSTEMS AND t-COVERS

A system of k-element subsets, $\mathcal{C}$, of an n-element underlying set V is called an (n,k,t)-*cover* if every t-subset $T \subset V$ is contained in some member of it, $T \subset C \in \mathcal{C}$. The minimum size of an (n,k,t)-cover is denoted by $C(n,k,t)$. A k-set covers exactly $\binom{k}{t}$

*E-mail addresses: zoltan@math.uiuc.edu and furedi@math-inst.hu
†E-mail address: h3361sze@ella.hu and gabors@math.bjsu.edu

© 1996 John Wiley & Sons, Inc.
CCC 1063-8539/96/010005-06
Journal of Combinatorial Designs, Vol. 4, No. 1 (1996)

t-sets, hence $C(n,k,t) \geq \binom{n}{t}/\binom{k}{t}$. This bound is best possible if every t-set is covered exactly once; in this case C is called an *(n,k,t)-Steiner system, $S(n,k,t)$*. Wilson [16] proved that there exists a Steiner system $S(n,k,2)$ if

$$\frac{n-1}{k-1} \text{ and } \frac{n(n-1)}{k(k-1)} \text{ are both integers} \tag{1}$$

and n is sufficiently large compared to $k, n > n_0(k)$. Equation (1) holds, e.g., when $n \equiv 1$ or $k (\bmod\ k^2 - k)$. Other well-known Steiner systems are the $S(q^2, q, 2)$ and $S(q^2 + q + 1, q + 1, 2)$, the so-called finite *affine* and *projective* planes (respectively); such planes exist if q is a prime power (see [9]).

Every element $v \in V$ of an (n,k,t)-cover must be contained in at least $C(n-1, k-1, t-1)$ members of C. This implies that $C(n,k,t) \geq (n/k)C(n-1, k-1, t-1)$, which together with the obvious $C(n,k,1) = \lceil n/k \rceil$ implies the so-called Schönheim bound [12]

$$C(n,k,t) \geq \left\lceil \frac{n}{k} \left\lceil \frac{n-1}{k-1} \cdots \left\lceil \frac{n-t+1}{k-t+1} \right\rceil \cdots \right\rceil \right\rceil = s(n,k,t). \tag{2}$$

Beside (1), there are several other cases when this bound is best possible. For example,

$$C(n,k,2) = s(n,k,2) \text{ if an } S(n-1,k,2) \text{ exists.} \tag{3}$$

Indeed, one gets $C(n,k,2) \leq C(n-1, k-1, 2) + \lceil (n-1)/(k-1) \rceil$ by adding appropriately $\lceil (n-1)/(k-1) \rceil$ new members through the nth element to an $(n-1, k, 2)$-cover. Another, isolated, example is

$$C(23,5,2) = s(23,5,2) = 28. \tag{4}$$

To prove (4) join the elements x, y to the vertex set of a finite projective plane on 21 vertices, and then add 7 more 5-tuples containing this pair. For $k = 3$, $t = 2$ equality holds in (2) for all n [8]), and for $k = 4$, $t = 2$ Mills [11] showed that $C(n,4,2) = s(n,4,2)$ for all $n \neq 7, 9, 10, 19$. (In the exceptional cases $C = s + 1$.)

2. THE LOTTERY PROBLEM

A system of k-element subsets, $\mathcal{L}$, of an n-element underlying set V is called an *(n,k,p,t)-Lottery system* if for every p-subset $P \subset V$ one can find a member $L \in \mathcal{L}$ with $|P \cap L| \geq t$. The minimum size of an (n,k,p,t)-Lottery system is denoted by $L(n,k,p,t)$. Obviously, $L(n,k,p,1) = \lceil (n-p+1)/k \rceil$. In this article we mainly deal with the case $t = 2$.

Cut the n-element set V into $p-1$ parts, $A_1, \ldots, A_{p-1}$, of sizes $a_1, \ldots, a_{p-1}$. Put an $(a_i, k, 2)$-cover to A_i. As every p-set in V meets an A_i in at least 2 elements, these families form a Lottery system, implying

$$L(n,k,p,2) \leq \min_{a_1 + \cdots + a_{p-1} = n} \left(C(a_1,k,2) + \cdots + C(a_{p-1},k,2) \right). \tag{5}$$

A theorem of Hanani, Ornstein, and T. Sós [10] states that

$$L(n,k,p,2) \geq \frac{n(n-p+1)}{k(k-1)(p-1)}. \tag{6}$$

This implies that equality holds in (5) if an $S(n/(p-1), k, 2)$ exists, for example (for large n) if $n \equiv p-1$ or $k(p-1)$ (mod $k(k-1)(p-1)$). Brouwer [3] proved that equality holds in (5) for all n if $k = p = 3$, namely, $L(2m + 1, 3, 3, 2) = C(m, 3, 2) + C(m + 1, 3, 2)$, $L(4m + 2, 3, 3, 2) = 2C(2m + 1, 3, 2)$, and $L(4m, 3, 3, 2) = C(2m + 1, 3, 2) + C(2m - 1, 3, 2)$. The aim of this article is to improve (6) thus to determine L for further infinite classes.

Theorem 1.

$$L(n,k,p,2) \geq \min_{a_1+\cdots+a_{p-1}=n} \frac{1}{k}\left(a_1\left\lceil \frac{a_1 - 1}{k - 1}\right\rceil + \cdots + a_{p-1}\left\lceil \frac{a_{p-1} - 1}{k - 1}\right\rceil\right) \tag{7}$$

The lower bound in the right-hand side of (7) is denoted by $l(n, k, p, 2)$. If $\lceil l(n, k, p, 2)\rceil$ equals to the upper bound in the construction (5), then we get equality.

Corollary 2. *Equality holds in (5) (and in Theorem 1) for*

(a) $n \equiv i(k - 1) + p - k \pmod{k(k - 1)(p - 1)}$, *for* $i = 1, 2, \ldots, p, n > n_0(k)$;

(b) $n \equiv i(k - 1) + (p - k) + (p - 1)\binom{k}{2} \pmod{k(k - 1)(p - 1)}$, *for* $i = 1, 2, \ldots, p, k \equiv 2 \pmod 4$, $n > n_0(k)$;

(c) $n \equiv i(k - 1) + p - k + 1 \pmod{k(k - 1)(p - 1)}$, *for* $i = 1, 2, \ldots, p, n > n_0(k)$;

(d) $n \equiv i(k - 1) + (p - k + 1) + (p - 1)\binom{k}{2} + 1 \pmod{k(k - 1)(p - 1)}$, *for* $i = 1, 2, \ldots, p, k \equiv 2 \pmod 4, n > n_0(k)$;

(e) $L(n, 3, 3, 2) = \lceil l(n, 3, 3, 2)\rceil$ *for* $n \not\equiv 9, 10 \pmod{12}$. *(Thus we almost got Brouwer's result);*

(f) $L(n, 4, 4, 2) = \lceil l(n, 4, 4, 2)\rceil$ *for* $n \equiv 0 - 15, 17, 34, 35 \pmod{36}$, $(n > n_0)$;

(g) $L(n, 5, 5, 2) = \lceil l(n, 5, 5, 2)\rceil$ *for* $n \equiv 4, 5, 8, 9, 12, 13, 16, 17, 20 \pmod{80}$ *for* $n > n_0$.

(h) $L(90, 5, 5, 2) = 100$.

The latest statement says that exactly 100 tickets needed to guarantee two correct matches in the Hungarian Lottery. Turán proved a lower bound 87, T. Nemetz 93, and V.T. Sós 97 (see in [10]), she also noted that $L(90, 5, 5, 2) \leq 102$. Of course, our result does not have too much practical importance. The probability of the event that a single ticket has two matches is exactly $1 - (\binom{n-k}{k} + k\binom{n-k}{k-1})/\binom{n}{k}$ which is about $k/2$-times larger then $1/L(n, k, k, 2)$. In the case $(n, k, p, t) = (90, 5, 5, 2)$, this means that *on average* about 43 tickets are needed to get two matches. (In another type of Hungarian (also Austrian) Lottery 6 numbers are selected randomly from 45 numbers. For this case $15 \geq L(45, 6, 6, 2) \geq 14 > 13 = \lceil l(45, 6, 6, 2)\rceil$. For the German, French, British, ... Lottery $19 \geq L(49, 6, 6, 2) \geq 16$.)

3. TURÁN'S THEOREM AND THE PROOF OF THEOREM 1

For a graph (or multigraph) G the number of edges is denoted by $e(G)$, the number of edges through a given vertex x (i.e., the *degree*), is denoted by $\deg_G(x)$. A graph G with vertex set V has p *independent* vertices, $\alpha(G) \geq p$, if some p-subset of V contains no edge. Turán [14] proved, that if G has n vertices and $\alpha(G) < p$, then

$$2e(G) \geq \min_{a_1+\cdots+a_{p-1}=n} (a_1(a_1 - 1) + \cdots + a_{p-1}(a_{p-1} - 1)), \tag{8}$$

moreover here equality holds if and only if G consists of $p - 1$ vertex-disjoint complete graphs of almost equal sizes. The right-hand side of (8) is at least $n(n - p + 1)/(p - 1)$.

The main tool of our proof is the following version of Turán's theorem, due to Erdős [7]. If $\alpha(G) < p$, then there exists a graph H on the same vertex set V consisting of $p - 1$ vertex disjoint copies of complete graphs such that

$$\deg_G(x) \geq \deg_H(x) \text{ for every } x \in V. \tag{9}$$

Since $2e(G) = \sum_{x \in V} \deg_G(x)$, (9) immediately implies (8). For a proof of (9) and for further extremal results see, e.g., Bollobás' book [2].

Lemma 3. *Let G be a multigraph on n vertices with $\alpha(G) < p$. Suppose that every degree is divisible by $k - 1$. Then*

$$2e(G) \geq \min_{a_1 + \cdots + a_{p-1} = n} (k-1)\left(a_1\left\lceil \frac{a_1 - 1}{k-1} \right\rceil + \cdots + a_{p-1}\left\lceil \frac{a_{p-1} - 1}{k-1} \right\rceil\right). \tag{10}$$

Proof of Lemma 3. Applying (9), we see that there exists a partition $A_1 \cup \cdots \cup A_{p-1}$ of the vertex set of G such that if a_i denotes $|A_i|$, then for every vertex $x \in A_i$ one has $\deg_G(x) \geq a_i - 1$. The divisibility property of the degree implies that $\deg_G(x) \geq (k-1)\lceil (a_i - 1)/(k-1) \rceil$, yielding (10). □

Proof of Theorem 1. Let $\mathcal{L}$ be an $(n, k, p, 2)$-Lottery system on the n-element set V. The set of pairs covered by the members of $\mathcal{L}$ defines a multigraph G (i.e., the multiplicity of $T \subset V$, $|T| = 2$ is the number of sets $L \in \mathcal{L}$ with $T \subset L$). The Lottery property is equivalent to the fact $\alpha(G) < p$. As the edge-set of G was obtained from $\mathcal{L}$, we have that

$$|\mathcal{L}| \binom{k}{2} = e(G), \tag{11}$$

moreover, $\deg_G(x)$ for an element $x \in V$ is exactly $(k - 1)$ times larger than the number of sets, L, with $x \in L \in \mathcal{L}$. One can apply Lemma 3 to G to get the desired lower bound for $|\mathcal{L}|$ from (11). □

Proof of the Corollaries. The function $f(x) = x\lceil x - 1/u \rceil$ ($u \geq 2$, integer) is not convex, but it is easy to minimize the right-hand side of (7) using the following two inequalities

$$f(x+1) + f(y-1) \leq f(x) + f(y) \text{ for integers } 0 < x + 1 \leq y \tag{12}$$

except whenever $(x - 1)/u$ is an integer,

$$f(x+u) + f(y-u) < f(x) + f(y) \text{ for } x + u < y. \tag{13}$$

Indeed, e.g., in case of (12) one gets $f(x) + f(y) - f(x+1) - f(y-1) = x(\lceil (x-1)/u \rceil - \lceil x/u \rceil) + (y-1)(\lceil (y-1)/u \rceil - \lceil (y-2)/u \rceil) + (\lceil (y-1)/u \rceil - \lceil x/u \rceil)$, and here all the three terms are nonnegative. Similarly, $f(x) + f(y) - f(x+u) - f(y-u) = (y - x - u) + u(\lceil (y-1)/u \rceil - \lceil (x-1)/u \rceil - 1)$, which is positive for $y > x + u$.

Repeatedly applying (12) and (13) one gets the following more explicit form. Write n as $n = a(p-1) + b(k-1) + c + (p-k)$, where a, b, c are nonnegative integers with $1 \leq b \leq p-1, 1 \leq c \leq k-1$. Then the right-hand side of (7) is minimized when the sequence $(a_1, \ldots, a_{p-1})$ consists of $b - 1$ times $a_i = a(k-1) + k$, once

$a_i = a(k-1) + 1 + c$ and the rest of them ($p - b - 1$ copies) equal to $a(k-1) + 1$. We get

$$L(a(k-1)(p-1) + b(k-1) + c + (p-k), k, p, 2) \geq \frac{1}{k}(an + (ba-1)(k-1) + bk + c) =: l(n,k,p,2) \quad (14)$$

One can apply (14) with $k = p = 5$, $(a,b,c) = (5,2,2)$ to get the lower bound $l(90,5,5,2) = 99.6$. The proofs of the cases (a)–(g) are similar easy calculations. The upper bounds are supplied by (1), (3), and (4), the exact results about $C(n,k,2)$ mentioned in the first section. □

4. FURTHER LOTTERY PROBLEMS

Brouwer and Voorhoeven [4] notes that the Hanani, Ornstein, T. Sós bound (6) naturally extends to the case $t > 2$

$$L(n,k,p,t) \geq T(n,p,t)/\binom{k}{t}, \quad (15)$$

where $T(n,p,t)$ (the *Turán number*) is the minimum number of t-sets such that every p-subset of an n-set contains at least one of them. The problem of determination of $T(n,p,t)$ is open for all $t > 2$; the best lower bound, due to de Caen [5], is $\binom{n}{t}\binom{p-1}{t-1}^{-1}((n-p+1)/(n-t+1))$. This and (15) give the following extension of (6)

$$L(n,k,p,t) \geq \frac{\binom{n}{t}}{\binom{p-1}{t-1}\binom{k}{t}} \times \frac{n-p+1}{n-t+1}. \quad (16)$$

The case $t > 2$ seems to be hopelessly difficult, for example for the German lottery it gives $L(49,6,6,3) \geq 87$. An "easy" upper bound is the following. In the Möbius plane of order q (Dembowski [6]) there are $q^2 + 1$ points, $q(q^2+1)$ circles, and each circle contains $q + 1$ points. Thus for $q = 5$, $q(q^2+1) = 130 = C(26,6,3)$, hence $L(49,6,6,3) \leq L(26+26,6,6,3) \leq 2 \cdot C(26,6,3) = 260$. A better upper bound due to Sterboul [12], is 175 (recent computer constructions gave 174, as the best bound we know). In the case of $n = 45$ we have got only $L(45,6,6,3) \geq 66$. For $n = 90$ formula (16) gives $L(90,5,5,3) \geq 1914$, while $C(45,5,3)$ is at least [by (2)], so an upper bound obtained by two (45, 5, 3)-covers consists of at least 2,970 tickets. For further designs that can help to solve lottery problems see Beth, Jungnickel, and Lenz [1].

ACKNOWLEDGMENTS

The research of the first author was supported in part by NSA. The research of the second author was supported in part by the Hungarian Science Foundation, Grant No. T 016237.

REFERENCES

[1] Th. Beth, D. Jungnickel, and H. Lenz, *Design theory,* Bibliographisches Institute, Zürich, 1985.

[2] B. Bollobás, *Extremal graph theory,* Academic Press, London-New York, 1978.

[3] A. E. Brouwer, *Some lotto numbers from an extension of Turán's theorem,* Math. Centre report 1978. MR82c: 05057

[4] A. E. Brouwer and M. Voorhoeven, *Turán theory and the Lotto problem,* Math. Centre Tracts **106** (1979), 99–105. (*Packing and covering in combinatorics,* A. Schrijver, (Editor), MR81b:05001).

[5] D. De Caen, *Extension of a theorem of Moon and Moser on complete subgraphs,* Ars Combin. **16** (1983), 5–10.

[6] P. Dembowski, *Finite geometries,* Springer, Berlin, 1968.

[7] P. Erdős, *On the graph theorem of Turán,* Mat. Lapok **21** (1970), 249–251 (in Hungarian). MR46 # 7090.

[8] M. K. Fort, Jr. and G. A. Hedlund, Minimal coverings of pairs by triples, *Pacific J. Math.* **8** (1958), 709–719.

[9] M. Hall, Jr., *Combinatorial theory,* Wiley, New York, 1967.

[10] H. Hanani, D. Ornstein, and V. T. Sós, On the lottery problem, *Magyar Tud. Akad. Mat. Kutató Int. Közl.* **9** (1964) 155–158. MR29 # 5479

[11] W. H. Mills, *On the covering of pairs by quadruples, I, II,* J. Combin. Theory Ser. A **13** (1972), 55–78, **15** (1973), 138–166.

[12] J. Schönheim, *On coverings,* Pacific J. Math. **14** (1964), 1405–1411.

[13] F. Sterboul, *Le problème du Loto, Proc. Colloq. Intern.* Mathematiques Discrètes: Codes et Hypergraphes, Brussels, 1978.

[14] P. Turán, *On an extremal problem in graph theory,* Mat. Fiz. Lapok **48** (1941), 436–452 (in Hungarian). Also see: *On the theory of graphs,* Colloq. Math. **3** (1954), 19–30.

[15] ——, *Research problems,* Magyar Tud. Akad. Mat. Kutató Int. Közl. **6** (1961), 417–423.

[16] R. M. Wilson, *On existence theory for pairwise balanced designs, I, II, III,* J. Combin. Theory Ser. A **13** (1972), 220–245, 246–273; **18** (1975), 71–79.

Received February 17, 1995
Accepted May 2, 1995