ACTA ARITHMETICA
VII (1961)

On caps of kind s in a Galois r-dimensional space

by

G. Tallini (Rome)

Summary. § 1. Introduction. § 2. The problem of embedding a $K^s_{r,q}$ in a cap of lower kind. § 3. On complete $K^s_{r,q}$ which cannot be embedded in a cap of kind two. § 4. The embedding of a complete $K^s_{r,q}$ in a cap of kind two. § 5. Construction of $K^s_{r,q}$ as intersection of caps of kind two. § 6. Further results about the embedding of a $K^s_{r,q}$ in a cap of lower kind.

§ 1. Introduction. In a *Galois space* $S_{r,q}$, i.e. in a projective r-dimensional space over a Galois field of order $q = p^h$ (where p, h are positive integers and p is a prime, the characteristic of the field) (1), a *K-cap* or cap of *order* K is a set of K distinct points, no three of which are collinear. We say that a *K-cap* is of *kind* s, and then we denote it by $K^s_{r,q}$, if any $s+1$ distincts of its points are *linearly independent*, but there are subsets of $s+2$ linearly dependent points; then, obviously, $2 \leqslant s \leqslant r$. Any such $K^s_{r,q}$ is said to be incomplete or complete, according as it is or not a subset of a $(K+1)^s_{r,q}$. Evidently, the space joining the points of a complete $K^s_{r,q}$ is $S_{r,q}$ itself, whence $K > r+1$.

The study of these caps is interesting from the algebraic-geometric point of view; moreover, some questions on their subject are deeply connected with information theory and statistics, as one can for example see from [1], [2].

The purpose of the present paper is to bring back the study of $K^s_{r,q}$ to that of complete caps of kind two (2). We begin by showing that, *with the only exception of some particular values for the pairs r, q, every $K^s_{r,q}$ is contained in a complete cap of kind two.* Further we proof that, *if $s \geqslant 4$, any $K^s_{r,q}$ is the complete intersection of a certain number of complete caps of kind two.* It follows that, from the knowledge of all complete caps of kind two of a Galois space, we can deduce immediately that of all $K^s_{r,q}$, if $s \geqslant 4$.

Finally, we deal with the more general problem of embedding a $K^s_{r,q}$ in a cap of a fixed kind, $t(< s)$, whence we draw significant limitations for the order K of a complete $K^s_{r,q}$.

(1) For further details cf., for example, [3], § 17.

(2) These caps have been already deeply investigated by B. Segre, especially in [4], [5], [6].

§ 2. The problem of embedding a $K^s_{r,q}$ in a cap of lower kind. A $K^s_{r,q}$ can never be contained in a cap of higher kind, since, by definition, $K^s_{r,q}$ contains $s+2$ dependent points. Therefore we may ask whether a $K^s_{r,q}(s\geqslant 3)$ may or may not be contained in a cap of lower kind, namely whether we can aggregate other points to those of $K^s_{r,q}$ so as to obtain a cap of kind $t<s$.

A first answer to the question is given by the following result:

Every $K^s_{r,q}$, with $s\geqslant 4$, is contained in a cap of kind $t\leqslant s-2$. It follows that every $K^s_{r,q}$ is contained in a complete cap of kind two or three.

For, let P be a point of an $(s-1)$-secant S_{s-2} of $K^s_{r,q}$, not belonging to any of the $\binom{s-1}{2}$ secants [3] of the cap $S_{s-2}\cap K^s_{r,q}$. Such a point P certainly exists, since $s\geqslant 4$. No line r through P can be a secant of $K^s_{r,q}$, since, otherwise, the space $S_{s-1}=r\cup S_{s-2}$ would contain $s+1$ points of $K^s_{r,q}$, which is excluded. Then, if we aggregate to the points of $K^s_{r,q}$ the point P, we obtain a $(K+1)$-cap. As this cap contains s dependent points (P and those of $S_{s-2}\cap K^s_{r,q}$) the cap is of kind $t\leqslant s-2$.

Further we have that:

Every incomplete $K^s_{r,q}$ is contained in a complete cap of kind two.

For, let us suppose $s\geqslant 3$ (if $s=2$ the property is evident) and let $H^s_{r,q}$ be a complete cap containing $K^s_{r,q}$. Further, let P be a point of $H^s_{r,q}$, but not of $K^s_{r,q}$, M_1 and M_2 any two points of $K^s_{r,q}$. Let us fix on the two distinct lines PM_1 and PM_2 two points N_1 and N_2 $(N_1,N_2\notin H^s_{r,q})$. Through N_i $(i=1,2)$ there is only the line PN_i meeting $H^s_{r,q}$ at two distinct points (because $H^s_{r,q}$ does not contain any four points lying on a plane, since $s\geqslant 3$) and therefore through N_i there is no secant of $K^s_{r,q}$. Besides, the line N_1N_2 is external to $K^s_{r,q}$ and so it follows that, by aggregating to the points of $K^s_{r,q}$ the points N_1 and N_2, we obtain a $(K+2)$-cap of kind two (since the set thus obtained contains the four points M_1,M_2,N_1,N_2 which lie on a plane), which is or complete or contained in a complete cap of kind two.

§ 3. On complete $K^3_{r,q}$ which cannot be embedded in a cap of kind two. The problem of embedding a complete $K^3_{r,q}$ in a cap of kind two seems to be exceptional with respect to other cases. In fact, we show that there exist complete $K^3_{r,q}$ not contained in any cap of kind two. Further, we give necessary conditions in order that this may happen.

Suppose that there exists a complete $K^3_{r,q}$ not contained in any cap of kind two. Through every point of $S_{r,q}-K^3_{r,q}$ there must be at least one secant of $K^3_{r,q}$ (for, if not, $K^3_{r,q}$, which is complete, would be contained in a cap of kind two), and exactly *one*, since, otherwise, $K^3_{r,q}$ would contain four points on a plane. It follows that the $\sum_{l=0}^{r}q^l-K$ distinct points of $S_{r,q}-K^3_{r,q}$ lie $q-1$ by $q-1$ on the $K(K-1)/2$ secants of $K^3_{r,q}$, whence

$$K^2(q-1)-K(q-3)-2\sum_{l=0}^{r}q^l=0\,. \tag{1}$$

From (1) it follows that

$$K=\frac{q-3+\sqrt{8q^{r+1}+q^2-6q+1}}{2(q-1)}\,. \tag{2}$$

Let us now denote by H_1 the number of points common to $K^3_{r,q}$ and to an arbitrarily chosen S_{r-1} of $S_{r,q}$. The points of S_{r-1} lying outside the secants of the H_1-cap $K^3_{r,q}\cap S_{r-1}$ are $\sum_{l=0}^{r-1}q^l-\binom{H_1}{2}(q-1)-H_1$ in number. Through each of them there is one, and only one, line meeting $K^3_{r,q}$ at two points not belonging to the above S_{r-1}. Those secants being $\binom{K-H_1}{2}$ in number, we obtain

$$\sum_{l=0}^{r-1}q^l-\binom{H_1}{2}(q-1)-H_1=\binom{K-H_1}{2}\,.$$

H_1 must therefore satisfy the equation

$$x^2q-x(2K+q-4)+\Big(K^2-K-2\sum_{l=0}^{r-1}q^l\Big)=0\,. \tag{3}$$

Equation (3)—as it can be easily proved—has always two real positive roots, whatever be K given by (2). In our case, moreover, these roots must be two integers. In fact, if (3) has only the integer root H_1, from the previous argument every hyperplane meets $K^3_{r,q}$ at the same number H_1, of points; but then also every S_{r-2} has in common with $K^3_{r,q}$ the same number, N, of points. In fact, equating the number of points of $K^3_{r,q}$, belonging to the $q+1$ hyperplanes through an arbitrarily chosen S_{r-2}, but outside it, to the number of points of $K^3_{r,q}$ not situated on the S_{r-2}, we obtain the equality

$$(H_1-N)(q+1)=K-N\,,$$

giving N univocally. Hence we could prove, inductively with respect to l, that every S_l $(l=r-1,r-2,\ldots,2,1)$ meets $K^3_{r,q}$ at the same number of points, which depends only upon l. But this is impossible, since there exist secants and tangents to $K^3_{r,q}$, whence our assertion.

[3] We call a line *secant* or *chord*, *tangent*, *external* of $K^s_{r,q}$ according as it contains two, one or no points of $K^s_{r,q}$.

Thus we have proved that:

A necessary condition for the existence of a complete $K^3_{r,q}$ *not contained in any cap of kind two, is that the second member of* (2) *is an integer, and that equation* (3) *has two* (*positive*) *integer roots* H_1 *and* H_2. *If such a* $K^3_{r,q}$ *exists, the hyperplanes of* $S_{r,q}$ *can be divided with respect to* $K^3_{r,q}$ *into two disjoint systems* (*each of them being not empty*), *according to whether they have* H_1 *or* H_2 *points in common with* $K^3_{r,q}$.

We observe that, for $r=3, q=2$ and $r=4, q=3$, the previous conditions are satisfied, being $K=5, H_1=3, H_2=1$ and $K=11$, $H_1=5, H_2=2$ respectively. Moreover, there effectively exist $5^3_{3,2}$ and $11^3_{4,3}$ not contained in any cap of kind two, as we shall now prove.

An example of such a $5^3_{3,2}$ is evidently given by the vertices of the fundamental tetrahedron and the unity point of an $S_{3,2}$; we can also easily see that every complete $K^3_{3,2}$ is projectively equivalent to such a $5^3_{3,2}$. An example of $11^3_{4,3}$ can be obtained as follows. In an $S_{4,3}$ of coordinates $(x_1, x_2, x_3, x_4, x_5)$, let us consider the vertices A_i $(i=1,\dots,5)$ of the fundamental simplex, the unity point U, and the points $B_1(0,1,-1,-1,1)$, $B_2(1,0,-1,1,-1)$, $B_3(1,1,0,-1,-1)$, $B_4(1,-1,-1,0,1)$, $B_5(1,-1,1,-1,0)$. These 11 points belong—as it can be easily seen—to the five following elliptic quadric cones $\mathcal{C}_i$ $(i=1,\dots,5)$, projecting from A_i the remaining 10 points respectively:

$$(4)\qquad \begin{cases} x_2x_3-x_2x_4-x_2x_5+x_3x_4-x_3x_5+x_4x_5=0\,,\\ x_1x_3-x_1x_4-x_1x_5-x_3x_4+x_3x_5+x_4x_5=0\,,\\ x_4x_1-x_4x_2-x_4x_5+x_1x_2-x_1x_5+x_2x_5=0\,,\\ x_2x_5-x_2x_1-x_2x_3+x_5x_1-x_5x_3+x_1x_3=0\,,\\ x_4x_3-x_4x_1-x_4x_2-x_3x_2+x_3x_1+x_2x_1=0\,. \end{cases}$$

It follows that those points constitute a 11-cap; and also that, if among them there exist four points on a plane, none of these can be an A_i $(i=1,\dots,5)$, therefore they will be four among the points U, B_i $(i=1,\dots,5)$: but it can be easily shown that the last points are four by four independent. Hence the 11-cap is a $11^3_{4,3}$. To prove that it is complete and not contained in any cap of kind two, it suffices to show that through every point P of $S_{4,3}-11^3_{4,3}$ there is one secant of $11^3_{4,3}$. Let $\mathcal{Q}$ be the elliptic quadric intersection of the cone $\mathcal{C}_1$ with the hyperplane $x_1=0$. Then $\mathcal{Q}$ is the projection from A_1 on $x_1=0$ of the 10 remaining points of $11^3_{4,3}$. If the point P belongs to $\mathcal{C}_1$, the property is evident; otherwise let $P'(\notin \mathcal{Q})$ be the projection from A_1 of P on $x_1=0$. Through P'—as it can be easily proved, being $q=3$—there are three secants of $\mathcal{Q}$, which, then, are the projection from A_1 of three secants of $11^3_{4,3}$. These secants meet the line A_1P at three distinct points, different from A_1, that is at the three points of A_1P different from A_1 (since $q=3$). One among the three secants must, then, contain P, and this completes the proof. Further—as it can be easily seen—we have that every $K^3_{4,3}$ of maximum order is projectively equivalent to the $11^3_{4,3}$ just considered.

We prove now that:

Given a $K^3_{r,q}$ *not contained in any cap of kind two, if* Q *is one arbitrarily chosen of its points, and we fix in any way a point outside* $K^3_{r,q}$ *on each of the* $K-1$ *secants issuing from* Q, *by aggregating the* $K-1$ *points thus obtained to those of* $K^3_{r,q}-Q$ *we obtain a complete* $[2(K-1)]^2_{r,q}$.

For, if three points P_i $(i=1,2,3)$ of the $[2(K-1)]$-set just considered are lying on a line r, the plane $Q\cup r$ must contain at least four points of $K^3_{r,q}$ (Q and the three further points intersected by the lines P_iQ on $K^3_{r,q}$), and this is impossible. The $[2(K-1)]$-set is therefore a $[2(K-1)]^2_{r,q}$; this is also complete, because through every point of $S_{r,q}-K^3_{r,q}$ there is a secant of $K^3_{r,q}$, which is evidently also a secant of $[2(K-1)]^2_{r,q}$.

From this result it follows the construction of a complete $20^2_{4,3}$, starting from the $11^3_{4,3}$ previously considered.

§ 4. The embedding of a complete $K^3_{r,q}$ in a cap of kind two. In the foregoing paragraph we have shown that, for particular values of r and q, there exist $K^3_{r,q}$ not contained in any cap of kind two. But such pairs of values are rather exceptional, as it is shown by the following results.

THEOREM. *Let us fix* r ($\geqslant 3$), *we can then determine an integer* q_r *such that, for every* $q>q_r$, *any* $K^3_{r,q}$ *is contained in a cap of kind two.*

First of all, we prove the theorem for $r=3$. Suppose that there exists a $K^3_{3,q}$ not contained in any cap of kind two. There are obviously 3-secants planes of $K^3_{3,q}$; moreover, if $q>2$, there are also planes meeting $K^3_{3,q}$ only at two distinct points: for, if not, each of the $q+1$ planes through a secant of $K^3_{3,q}$ has a further point in common with the cap, so that $K=q+3$, and by (1), $q^3-2q^2-q+2=0$, which contradicts the hypotesis $q>2$. Then we have (cf. § 3, first proposition) $H_1=3$, $H_2=2$; from (3) we also have $H_1+H_2=(2K+q-4)/q=5$, that is $K=2(q+1)$, and by (1), $q^3-q=0$, which is impossible, since $q>2$. It follows that

every $K^3_{3,q}$, *with* $q>2$, *is contained in a cap of kind two*.

Let us now prove the theorem for $r\geqslant 4$. We begin by establishing the following

LEMMA. *Let us fix an integer* $r\geqslant 4$, *an index* $i(2\leqslant i\leqslant r-1)$, *two polynomials* $f_i(x)$ *and* $g_i(x)$ *with integer coefficients, and an integer constant* a_i. *If, for an integer* $q>0$, *it is possible to find an integer* s_i *such that*

$$(5)_i\qquad s_i^2q^i(q-1)+s_i[qf_i(q)-1]+[qg_i(q)-a_i]-2(q^{r-i}+\dots+q+1)=0\,,$$

then it must be $s_i = -(2+a_i)+qs_{i+1}$, *where* s_{i+1} *is an integer such that*

$$(5)_{i+1} \quad s_{i+1}^2 q^{i+1}(q-1)+s_{i+1}[qf_{i+1}(q)-1]+ \\ +[qg_{i+1}(q)-a_{i+1}]-2(q^{r-(i+1)}+\ldots+q+1)=0,$$

where a_{i+1}, $f_{i+1}(x)$, $g_{i+1}(x)$ *are an integer constant and two polynomials with integer coefficients respectively, which can be expressed by means of* a_i, $f_i(x)$, $g_i(x)$.

From $(5)_i$, s_{i+1} denoting an integer, we have immediately $s_i = -(2+a_i)+qs_{i+1}$. Substituting this expression in $(5)_i$, we get $(5)_{i+1}$, where

$$f_{i+1}(q) = f_i(q)-2(a_i+2)q^{i-1}(q-1),$$
$$g_{i+1}(q) = (a_i+2)^2q^{i-2}(q-1)-\frac{f_i(q)-f_i(0)}{q}(a_i+2)+\frac{g_i(q)-g_i(0)}{q},$$
$$a_{i+1} = f_i(0)(a_i+2)-g_i(0).$$

Thus the lemma is proved.

Let us now fix $r \geqslant 4$, and suppose that there exist, for a given $q>2$ (q even or odd), a $K^3_{r,q}$ not contained in any cap of kind two. By virtue of § 3, both the roots H_1, H_2 of equation (3) must be integers, whence, as $H_1+H_2 = (2K+q-4)/q$ and $H_1\cdot H_2 = \big(K^2-K-2\sum_{l=0}^{r-1}q^l\big)/q$, we have:

$$\begin{cases} 2(K-2) \equiv 0 \ (\mathrm{mod}\, q), \\ K^2-K-2 = (K+1)(K-2) \equiv 0 \ (\mathrm{mod}\, q). \end{cases}$$

From these relations it follows that (since $q>2$) $K = 2+s_1q$ (where s_1 is an integer); besides, since K must satisfy (1), we have $s_1 = s_2q$ (s_2 an integer), so that $K = 2+s_2q^2$. Substituting this expression in (1) we get

$$s_2^2q^2(q-1)+s_2(3q-1)-2(q^{r-2}+\ldots+q+1) = 0.$$

This relation coincides with $(5)_i$ for $i=2$, where $f_2(x)=3$, $g_2(x)=0$ and $a_2=0$. Then, from the lemma, and proceeding inductively with respect to i, we obtain, on putting $b_i = -(2+a_i)$:

$$s_2 = b_2+q\{b_3+q\{\ldots+q[b_{r-2}+q(b_{r-1}+qs_r)]\ldots\}\}.$$

Then we get

$$(6) \qquad K = s_rq^r+b_{r-1}q^{r-1}+\ldots+b_2q^2+2,$$

where s_r is an integer dependent on q and $b_i = -(2+a_i)$ are integers which do not depend either on q or on r, and which can be determined inductively with respect to i by virtue of the lemma.

From (2) and (6), recalling that $q \geqslant 3$ and $r \geqslant 4$, we easily get that, as soon as

$$q > q^* = \left[\tfrac{5}{4}\mathrm{Max}(|b_2|,\ldots,|b_{r-1}|)+1\right] \ (^4),$$

(4) If a is a real number, we denote by $[a]$ the integral part of a.

we have $|s_r|<1$ and so $s_r = 0$. Therefore (6) becomes

$$K = b_{r-1}q^{r-1}+\ldots+b_2q^2+2.$$

On substuting this expression in (1) we get

$$(7) \quad (b_{r-1}q^{r-1}+\ldots+b_2q^2+2)^2(q-1) = \\ = (b_{r-1}q^{r-1}+\ldots+b_2q^2+2)(q-3)+2\sum_{l=0}^{r}q^l.$$

Equality (7) is not an identity in q (for, otherwise, its left-hand side should be a polynomial in q of degree r, with leading coefficient 2, and so $r = 2t+1$ and $b_{r-1} = \ldots = b_{t+1} = 0$, $b_t^2 = 2$; but this is impossible, b_t being an integer). Consequently, if $q>q^*$, q must be a solution of equation (7). Then, if we denote by q_r the maximum between q^* and the greatest integer root of (7), we conclude with the theorem.

An easy calculation shows that the foregoing q_r, for $r=4$, is equal to 11; further, we get that for $q \neq 3$ and $q \leqslant 11$ the right-hand side of (2) is never integer. Hence we deduce that:

Every $K^3_{4,q}$, *with* $q\neq 3$, *must be contained in a cap of kind two.*

We now prove that:

Every $K^3_{r,q}$, *with* $q=2^h$, $h\geqslant 3$, $r\geqslant 4$ *and* $hr+h+3 = 2n$, *must be contained in a cap of kind two.*

It suffices to show that, under the hypoteses above, the discriminant $\Delta(q) = 8q^{r+1}+q^2-6q+1$ of (1) is never a square. For, on supposing $\Delta(q) = a^2$ (a positive integer), we have (since $q\geqslant 8$):

$$(a+2^n)(a-2^n) = a^2-8q^{r+1} = q^2-6q+1 > 1,$$

whence $(a-2^n)\geqslant 1$, and so:

$$2^n < (a+2^n)(a-2^n) = q^2-6q+1 < 2^{2h}.$$

But this relation is absurd, since at present $n>2h$.

We have, moreover, that:

Every $K^3_{2n,2}$ *is contained in a cap of kind two.*

For, if we suppose the discriminant of (1) $\Delta(2) = 2^{2(n+2)}-7 = a^2$ (where a is a positive integer), we get

$$2^{n+2} < (2^{n+2}+a)(2^{n+2}-a) = 2^{2(n+2)}-a^2 = 7,$$

and this is impossible.

§ 5. Construction of a $K^s_{r,q}$ as intersection of caps of kind two. From the previous results we see that in a space $S_{r,q}$ corresponding to a general choice of q, every cap of kind three—and so every $K^s_{r,q}$

(cf. § 2)—is contained in a cap of kind two. Our purpose is now to show that:

In such an $S_{r,q}$, every $K^s_{r,q}$, with $s \geq 4$, is the complete intersection of h caps of kind two, where, if $q > 2$,

$$h \geq \frac{q^{s-2}+\ldots+q+1-(s-1)-(q-1)\binom{s-1}{2}}{q^{s-3}-s+3} \tag{8}$$

so that $h \geq q+1$ when q is sufficiently large with respect to s.

Let h (>0) denote the number of all the caps of kind two which contain a given $K^s_{r,q}$. If the result is not true, then these caps meet in a point P not belonging to $K^s_{r,q}$. Let P_1 be a point of $K^s_{r,q}$. The line PP_1 is a tangent of $K^s_{r,q}$ at P_1 (for, if not, each of the h caps just considered should contain three collinear points). Let Q ($\neq P, P_1$) be a point of PP_1. Then Q cannot belong to any of the h caps, and so there is a line through it meeting $K^s_{r,q}$ at two distinct points, P_2, P_3 say. If R ($\neq P, P_2$) is a point of PP_2, through R also there must be a line meeting $K^s_{r,q}$ at two distinct points, P_4, P_5 say. Consequently, the S_3 joining the points P, P_1, P_2, P_4 must contain the 5 points P_i ($i = 1, \ldots, 5$) of $K^s_{r,q}$, and this is impossible, since $s \geq 4$.

Let us now fix an $(s-1)$-secant S_{s-2} of $K^s_{r,q}$. Through each of its $q^{s-2}+\ldots+q+1-\binom{s-1}{2}(q-1)-(s-1)$ points, not belonging to the $\binom{s-1}{2}$ secants of the cap $S_{s-2} \cap K^s_{r,q}$, there cannot be any secant line of $K^s_{r,q}$ (for, if not, the S_{s-1} joining S_{s-2} and such a secant, should contain $s+1$ points of $K^s_{r,q}$). Then, through each of those points there is at least one of the h caps, on the other hand each of these caps meets S_{s-2} in at most $q^{s-3}-q+3$ points, if $q>2$, distinct from those of $K^s_{r,q}$ (5). It must therefore be

$$(q^{s-3}-s+3)h \geq q^{s-2}+\ldots+q+1-\binom{s-1}{2}(q-1)-(s-1),$$

whence (8) follows at once.

§ 6. Further results about the embedding of a $K^s_{r,q}$ in a cap of lower kind. Let us fix a $K^s_{r,q}$ ($s \geq 2$) and, for every integer $t \leq s$, denote by N_t the number of points of $S_{r,q}$ through which there is at least a t-secant S_{t-1} of $K^s_{r,q}$. We shall prove that

$$N_t \leq \binom{K}{t}(q-1)^{t-1}+\binom{K}{t-1}(q-1)^{t-2}+\ldots+\binom{K}{2}(q-1)+K, \tag{9}$$

where the equality sign holds if and only if through every point of $S_{r,q}$ lying outside each $(l-1)$-secant S_{l-2} of $K^s_{r,q}$, there is at most an l-secant S_{l-1} of $K^s_{r,q}$, for $l = 2, \ldots, t$.

(5) We recall that the greatest number of points of $S_{t,q}$ ($t \geq 2$, q odd or even, $q > 2$) three by three non collinear is $\leq q^{t-1}+2$ (cf. [7], p. 124).

For, the points of an S_{l-1} not lying on any face of one of its l-simplexes are evidently $(q-1)^{l-1}$ in number. Therefore, the points of the $\binom{K}{l}$ l-secants S_{l-1} of $K^s_{r,q}$ which do not lie on any face of the l-simplexes $S_{l-1} \cap K^s_{r,q}$ are n_l in number, where $n_l \leq \binom{K}{l}(q-1)^{l-1}$, the equality holding if and only if the hypotesis of the proposition is satisfied. Our statement follows on adding the limitations just obtained, for $l = t, t-1, \ldots, 2, 1$.

Evidently we have also that:

If t ($\leq s$) is any positive integer, a necessary and sufficient condition in order that a $K^s_{r,q}$ is not properly contained in any cap of kind $h = t, t+1, \ldots, s$ is that every point of $S_{r,q}$ lies on at least a t-secant S_{t-1} of $K^s_{r,q}$, i.e., that $N_t = q^r+\ldots+q+1$.

From this last result and by virtue of (9), it follows that:

If a $K^s_{r,q}$ is not properly contained in any cap of kind $h = t, t+1, \ldots, s$, then

$$q^r+\ldots+q+1 \leq \binom{K}{t}(q-1)^{t-1}+\binom{K}{t-1}(q-1)^{t-2}+\ldots+\binom{K}{2}(q-1)+K. \tag{10}$$

On putting in (10) $t = s$ we have that, *for a complete $K^s_{r,q}$ it must be*

$$q^r+\ldots+q+1 \leq \binom{K}{s}(q-1)^{s-1}+\binom{K}{s-1}(q-1)^{s-2}+\ldots+\binom{K}{2}(q-1)+K. \tag{11}$$

Let us now suppose for $K^s_{r,q}$ $s \geq 3$ and put $\sigma = [(s+1)/2]$; then, *if $l = 2, \ldots, \sigma$, through every point P of $S_{r,q}$, not lying on any $(l-1)$-secant S_{l-2} of $K^s_{r,q}$, there is at most an l-secant S_{l-1} of $K^s_{r,q}$.* For, if through P there are two such spaces, S'_{l-1} and S''_{l-1} say, their intersection S_i ($i \geq 0$, since $P \in S_i$) must have in common with $K^s_{r,q}$ at most i points (for, if not, P must belong to an $(i+1)$-secant S_i of $K^s_{r,q}$, and so to an $(l-1)$-secant S_{l-2} of $K^s_{r,q}$). Then the space $S_{2l-2-i} = S'_{l-1} \cup S''_{l-1}$ meets $K^s_{r,q}$ at least in $2l-i$ distinct points, which must therefore be dependent and so $2l-i > s+1$. But this is impossible, since $2l-i \leq s+1$, being $l \leq \sigma = [(s+1)/2] \leq (s+1)/2$ and $i \geq 0$. By virtue of the first result of the present § 6, we then have that, if $t \leq \sigma$, the equality sign must hold in (9). Since $N_t \leq q^r+\ldots+q+1$, on putting

$$D(t, r, q, K) = q^r+\ldots+q+1-\left[\binom{K}{t}(q-1)^{t-1}+\ldots+\binom{K}{2}(q-1)+K\right],$$

it follows that *for a $K^s_{r,q}$ ($s \geq 3$) we have*

$$D(t, r, q, K) \geq 0, \quad t \leq \sigma = \left[\frac{s+1}{2}\right]. \tag{12}$$

We observe that

$$D(2, r, q, K) > D(3, r, q, K) > \ldots > D(\sigma, r, q, K),$$

whence for a $K^s_{r,q}$ $(s \geqslant 3)$ by virtue of (12) at most $D(\sigma, r, q, K)$ may be zero. Hence, being $D(t, r, q, K) = q^r + \ldots + q + 1 - N_t$, if $t \leqslant \sigma$, and by virtue of second result of the present § 6, we obtain that:

Given any $K^s_{r,q}$ $(s \geqslant 3)$, *only two cases may occur*:

(I) $D(\sigma, r, q, K) > 0$, *and then* $K^s_{r,q}$ *is properly contained in at least one cap of kind* h, *where* $\sigma \leqslant h \leqslant s$.

(II) $D(\sigma, r, q, K) = 0$, *and then* $K^s_{r,q}$ *is not properly contained in any cap of kind* $h = \sigma, \ldots, s$ (*and so* $s \neq 4$, *cf. first result* § 2); *but, if* $s \geqslant 5$, $K^s_{r,q}$ *is contained in a cap of kind* $\sigma - 1$ (*because then* $\sigma - 1 \geqslant 2$ *and* $D(\sigma - 1, r, q, K) > 0$).

If $a^t_{r,q}$ denotes the least positive integer x satisfying

$$\binom{x}{t}(q-1)^{t-1} + \ldots + \binom{x}{2}(q-1) + x - (q^r + \ldots + q + 1) \geqslant 0\,;$$

since for a complete $K^s_{r,q}$ both (11) and (12) must hold, we have

$$a^s_{r,q} \leqslant K \leqslant a^\sigma_{r,q}\,. \tag{13}$$

We have—as it can be easily proved—that

$$\lim_{q\to\infty} \frac{(a^t_{r,q})^t}{t!\, q^{r-t+1}} = 1\,. \tag{14}$$

Then from (13) we see that, for any complete $K^s_{r,q}$ having q sufficiently large with respect to r, we have

$$\sqrt[s]{s!-1}\, q^{(r-s+1)/s} \leqslant K \leqslant \sqrt[\sigma]{\sigma!+1}\, q^{(r-\sigma+1)/\sigma}\,. \tag{15}$$

References

[1] R. C. Bose, *Mathematical theory of the symmetrical factorial design*, Sankhyà (8) 2 (1947), pp. 107-116.

[2] — and D. K. Ray Chaudhuri, *On a class of error correcting binary group codes*, Inst. of statistics Univ. of North Carolina, Mimeograph. series, n. 240 (1959).

[3] B. Segre, *Lezioni di Geometria Moderna*, vol. I, Bologna, Zanichelli, 1948.

[4] — *On Galois geometries*, Proc. of Internat. Congress of Math., 1958, 3, pp. 488-499.

[5] — *Le geometrie di Galois*, Ann. di Mat. (4) 48 (1959), pp. 1-97.

[6] — *On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two*, Acta arithmetica 5 (1959), pp. 315-332.

[7] G. Tallini, *Sulle K-calotte di uno spazio lineare finito*, Ann. di Mat. (4) 42 (1956), pp. 119-164.

Reçu par la Rédaction le 22. 12. 1960

ACTA ARITHMETICA
VII (1961)

Unitary products of arithmetical functions

by

E. Cohen (Knoxville, Tenn.)

1. Introduction. In this paper n and r will represent positive integers. The *unitary product* (convolution) $q(n)$ of two arithmetical functions $f(n), g(n)$ was defined in an earlier paper [1] by

$$q(n) = \sum_{\substack{d\delta = n \\ (d,\delta)=1}} f(d)g(\delta)\,, \tag{1.1}$$

where the summation is over all relatively prime pairs d, δ such that $d\delta = n$, that is, over all complementary pairs d, δ of unitary divisors of n. If the condition, $(d, \delta) = 1$, is removed, the summation in (1.1) becomes the ordinary *Dirichlet* (or *direct*) *product* of the functions $f(n), g(n)$.

In [1] the unitary product was used in treating several asymptotic problems in elementary number theory. It is the purpose of the present paper to apply this method to additional problems involving the distribution of sets of integers. We shall use a generalized unitary inversion formula proved in § 3 (Theorem 2.3).

Let n have distinct prime factors $p_1, \ldots, p_t$, and place

$$n = p_1^{e_1} \ldots p_t^{e_t}\,, \tag{1.2}$$

so that $t = 0$ in case $n = 1$. Suppose a and b to be positive integers. We denote by $S_{a,b}$ the set of integers n in (1.2) such that each e_i is divisible by either a or b, and by $S^*_{a,b}$ the set of n such that each e_i is divisible by one of the integers a, b, but not by both $(i = 1, \ldots, t)$. For real x, $S_{a,b}(x)$ and $S^*_{a,b}(x)$ will denote the number of $n \leqslant x$ contained in $S_{a,b}$ and $S^*_{a,b}$, respectively. Asymptotic representations of $S_{a,b}(x)$ and $S^*_{a,b}(x)$ are deduced in § 4 under certain natural conditions on a and b.

Our investigation of the distribution of $S_{a,b}$ and $S^*_{a,b}$ involves the consideration of two divisor functions, $\tau_{a,b}(n)$ and $\tau^*_{a,b}(n)$, defined as follows: $\tau_{a,b}(n)$ is the number of decompositions of n in the form $n = d^a\delta^b$, while $\tau^*_{a,b}(n)$ denotes the number of such decompositions, under the