A PROOF OF THE THEOREM ACCORDING TO WHICH EVERY PRIME NUMBER POSSESSES PROPERTY B

CHRISTIAN REIHER

Abstract. In the present thesis, we prove a conjecture belonging to a subbranch of additive combinatorics that is called combinatorial zero–sum theory. Denoting by p an arbitrary prime number, it has been known for about forty years that every sequence $(P_1, P_2, \dots, P_{2p-1})$ consisting of $2p-1$ points from the affine plane $\mathbb{F}_p^2$ possesses a non–empty subsequence the sum of whose elements equals zero. This fact has first been shown independently by Kruyswijk and Olson and is nowadays known to be an easy consequence of Alon's combinatorial Nullstellensatz. A less obvious question asks for a classification of all those sequences $(P_1, P_2, \dots, P_{2p-2})$ of length $2p-2$ whose only zero–sum subsequence is the empty one. This problem has been investigated by several researchers and in this respect a certain conjecture implying in particular that any such sequence contains $p-2$ equal points has attracted a great deal of attention in recent years. A precise version of this conjecture will be given below. By definition, the prime number p has property B if and only if it behaves in accordance with the conjecture under discussion; by developing for the first time a powerful method for tackling such inverse problems over $\mathbb{F}_p^2$, we prove the result alluded to in the title.

1. Introduction.

The main objective of this paper is a thorough discussion of a certain problem belonging to that subfield of additive combinatorics which is called combinatorial zero–sum theory. For its motivation it seems useful to recollect three well known related results. Fix an arbitrary prime number p.

Fact 1. Suppose that a sequence $a_1, a_2, \dots, a_p$ from $\mathbb{F}_p$, i.e. the field of residue classes of integers modulo p, is given. Then there exists a non–empty set $I \subseteq \{1, 2, \dots, p\}$ of indices such that $\sum\limits_{i \in I} a_i = 0$.

The number p of terms required to appear in the given sequence cannot be replaced by $p-1$ as the counterexample provided by the sequence all of whose terms are equal to 1 exemplifies. It can be shown, however, that this is essentially the only such example, or to be more precise:

2000 *Mathematics Subject Classification.* Primary: 05E15, 11P70. Secondary: 11B50.

Key words and phrases. Combinatorial zero–sum theory, planar lattice points, inverse Davenport problem, property B.

Fact 2. For any sequence $a_1, a_2, \dots, a_{p-1}$ of elements from $\mathbb{F}_p$ exactly one of the following two alternatives occurs:

(a) There is a non–empty $I \subseteq \{1, 2, \dots, p-1\}$ satisfying $\sum\limits_{i \in I} a_i = 0$.
(b) For some non–zero $k \in \mathbb{F}_p$ we have $a_1 = a_2 = \dots = a_{p-1} = k$.

As usual, one can make matters harder by attempting to generalize what one has just considered to a setting involving higher dimensions. Thus, you may pretend to be curious about the corresponding situation in the affine plane $\mathbb{F}_p^2$ viewed as a vector space over $\mathbb{F}_p$ and then ask about the minimal number of terms a sequence of points needs to contain in order to enforce for reasons of its mere length the existence of a non–empty zero–sum subsequence. Here a theorem discovered independently by Kruyswijk and Olson (see [2] and [12]) comes in handily, which implies, among other things:

Fact 3. Given any sequence $P_1, P_2, \dots, P_{2p-1}$ of points from $\mathbb{F}_p^2$, there exists a non–empty set $I \subseteq \{1, 2, \dots, 2p-1\}$ of indices such that $\sum\limits_{i \in I} P_i = 0$.

We defer the proof this statement to the end of this section, so the reader not familiar with it is kindly asked to just believe it for a while. It is important to notice that again, we cannot replace the number $2p-1$ occurring here by $2p-2$ as, e.g., the sequence whose first $p-1$ terms equal $(0, 1)$ and whose last $p-1$ terms equal $(1, 0)$ witnesses. So once more the question concerning all such examples emerges but as we shall now explain it is going to be substantially more difficult this time.

Let us for the sake of discussion agree to call a sequence of $2p-2$ points $(P_1, P_2, \dots, P_{2p-2})$ *suspicious* if except for $I = \emptyset$ there is no $I \subseteq \{1, 2, \dots, 2p-2\}$ for which $\sum\limits_{i \in I} P_i = 0$. To clarify our understanding of the structure of all suspicious sequences, it is helpful to consider operations applicable to sequences of points that preserve suspiciousness. Plainly, every permutation of the involved terms has this property. Moreover for any automorphism φ of the vector space $\mathbb{F}_p^2$, the map

$$(P_1, P_2, \dots, P_{2p-2}) \longmapsto (\varphi P_1, \varphi P_2, \dots, \varphi P_{2p-2})$$

constitutes another such operation. We now call two suspicious sequences *isomorphic* if they are mutually obtainable from one another by a certain combination of the transformations just described and hence, for easy commutativity reasons, also by a single permutation followed by an automorphism.

For instance, what we have really alluded to when giving the above example is that any sequence involving each of two linearly independent points exactly $p-1$ times has to be suspicious. In awareness of this, it is natural to wonder whether there are more such sequences and a moments reflection reveals that indeed there are some more subtle ones: First, taking $p-1$ times the point $(1,0)$ and moreover $p-1$ points of the form $(a,1)$ in an arbitrary fashion, it is easy to verify that we also obtain a suspicious sequence. We say that a sequence isomorphic to any of the ones just described is of the *first type*. Second, taking the point $(1,0)$ only $p-2$ times and then p points of the form $(a,1)$ the sum of which is also $=(1,0)$ we get another class of suspicious sequences and any sequence isomorphic to one of these is said to be of the *second type*. Of course, in extreme cases a suspicious sequence can be of both types at the same time, but this circumstance is rather immaterial to what follows. More relevantly, no other examples of suspicious sequences have hitherto been discovered and it is widely believed that there are none. The prime number p is said to have *property B* if it behaves in accordance with that conjecture and using this terminology the principal result proved in the following pages reads

($\boxplus$) *Every prime number has property B.*

The reader may amuse himself for a few minutes time by verifying directly that 2 and 3 do indeed have property B, though as we shall see in Example 2.7 below a fairly modest amount of theory suffices to almost trivialize these two small cases.

Another way of looking at the whole problem involves the notion of a *cloudy* sequence, by which we mean any sequence $(P_1, P_2, \ldots, P_{2p-1})$ of length $2p-1$ such that apart from $I=\emptyset$ there is no $I \subsetneqq \{1,2,\ldots,2p-1\}$ such that $\sum\limits_{i\in I} P_i = 0$. Note that by Fact 3 this can only occur if $P_1+P_2+\ldots+P_{2p-1}=0$. Plainly, every cloudy sequence can be made suspicious by deleting any of its terms and conversely a suspicious sequence $(P_1, P_2, \ldots, P_{2p-2})$ can be cloudified by inserting the point $-(P_1+P_2+\ldots+P_{2p-2})$ at an arbitrary place. Thus, property B can equivalently be viewed as a classification of cloudy sequences, and working the details out one discovers that thereby the two types introduced above unify into a single concept. More explicitly, we call a sequence of $2p-1$ points *simple* provided that it is, in the same sense as above, isomorphic to one that contains $p-1$ times the point $(1,0)$ and p further points each of which is of the form $(a,1)$ and that sum up to $(1,0)$. Then p has property B if every cloudy sequence is simple. Another convenient reformulation of property B, that likewise belongs to the folklore of the subject, will be given in Observation 2.6. —

Let us mention some recent partial results towards ($\boxplus$), though none of them will be relied upon in what follows. Arguably the morally most satisfying of these has been obtained by the authors of [3], who have shown with the help of a computer that up to 23 every prime number has property B, so the chances that ($\boxplus$) failed have been negligible ever since we started to think about the problem. In the same paper, it has also been proved that if the positive real number δ is chosen sufficiently small, e.g. $\delta = 4\times 10^{-7}$, then every suspicious sequence contains one point with multiplicity at least δp, and plenty of other statements pertaining to the three highest multiplicities with which points appear in hypothetical counterexamples have been established there as well. There are also quite a lot of papers that at some point just assume ($\boxplus$) to be true and derive interesting consequences (see e.g. [2], [4], [5], [6] and [14]). In our final section, we have collected some of the more spectacular ones among these applications.

As promised, we now give a quick

Proof of Fact 3. Let $P_i = (a_i, b_i)$ for all $i \in [2p-1]$, take $2p-1$ variables $\eta_1, \eta_2, \dots, \eta_{2p-1}$, set

$$A = \sum_{1 \leqslant i \leqslant 2p-1} a_i \eta_i, \qquad B = \sum_{1 \leqslant i \leqslant 2p-1} b_i \eta_i$$

and finally

$$Q = \prod_{1 \leqslant i \leqslant 2p-1} (1 - \eta_i) - (1 - A^{p-1})(1 - B^{p-1}).$$

The total degree of Q, viewed as a member of the ring $\mathbb{F}_p[\eta_1, \eta_2, \dots, \eta_{2p-1}]$ of polynomials is $2p-1$ and the coefficient accompanied by which the monomial $\eta_1 \eta_2 \cdot \ldots \cdot \eta_{2p-1}$ occurs is $(-1)^{2p-1}$ and thus in particular non vanishing. Invoking the Combinatorial Nullstellensatz from [1], we find values $\eta_i \in \{0, 1\}$ such that $Q \neq 0$ and setting $I = \{i \in [2p-1] \mid \eta_i = 1\}$ it is straightforward to see that $I \neq \emptyset$ and hence $A = B = 0$, wherefore I is as desired. □

2. Some initial observations.

Repeating the argument just given, we can deduce something about suspicious sequences as well. But before doing so, it seems advisable to introduce the following

Definition 2.1. Let F denote any field of characteristic p and m, n two non negative integers. Given any sequence $P_1, P_2, \dots, P_{m+n}$ of $m+n$ points from F^2, say $P_i = (a_i, b_i)$ for all $i \in [m+n]$, we set

$$\mu_m(P_1, P_2, \dots, P_{m+n}) = \sum_{\substack{M \cup N = [m+n] \\ |M| = m, |N| = n}} \prod_{i \in M} a_i \prod_{j \in N} b_j.$$

In the particular case where exactly $2p-2$ points are involved and $m = n = p-1$, we simply write μ in place of μ_{p-1}.

Observation 2.2. *If φ denotes an automorphism of F^2 and D its determinant, then for all $P_1, P_2, \dots, P_{2p-2} \in F^2$ we have*

$$\mu(\varphi P_1, \varphi P_2, \dots, \varphi P_{2p-2}) = D^{p-1} \mu(P_1, P_2, \dots, P_{2p-2}).$$

Proof. Fix the sequence $(P_1, P_2, \dots, P_{2p-2})$ and consider φ as varying. If the claim is already known for two automorphisms φ and φ', then by multiplicativity of determinants it follows to hold for their product $\varphi\varphi'$ as well. Hence it suffices to verify the above identity in those cases, where either φ is of the form $(x, y) \longmapsto (kx, y)$ for some $k \in F^\times$ or given by $(x, y) \longmapsto (y, x)$ or by $(x, y) \longmapsto (x+y, y)$. The first two of these alternatives offer no difficulty, so we restrict our attention to the third one. Let $P_i = (a_i, b_i)$ and $Q_i = (a_i + b_i, b_i)$ for all $i \in [2p-2]$. Then

$$\mu(Q_1, Q_2, \dots, Q_{2p-2}) = \sum_{0 \leqslant i \leqslant p-1} \binom{2p-2-i}{p-1} \mu_i(P_1, P_2, \dots, P_{2p-2})$$

and taking into account that except for the last one all binomial coefficients appearing here are divisible by p, we get

$$\mu(Q_1, Q_2, \dots, Q_{2p-2}) = \mu(P_1, P_2, \dots, P_{2p-2})$$

as claimed. □

The additional generality gained by admitting possibilities other than $F = \mathbb{F}_p$ will become exploited at the end of our next section.

Lemma 2.3. *If the sequence $(P_1, P_2, \dots, P_{2p-2})$ of points from $\mathbb{F}_p^2$ is suspicious, then*

$$\mu(P_1, P_2, \dots, P_{2p-2}) = 1.$$

Proof. Again let $P_i = (a_i, b_i)$ for $i = 1, 2, \dots, 2p-2$, then take $2p-2$ variables $\eta_1, \eta_2, \dots, \eta_{2p-2}$ and set

$$A = \sum_{1 \leqslant i \leqslant 2p-2} a_i \eta_i, \quad B = \sum_{1 \leqslant i \leqslant 2p-2} b_i \eta_i$$

as well as

$$Q = \prod_{1 \leqslant i \leqslant 2p-2} (1 - \eta_i) - (1 - A^{p-1})(1 - B^{p-1}).$$

By hypothesis, we have $Q(\eta_1, \eta_2, \dots, \eta_{2p-2}) = 0$ whenever the values of the involved variables are chosen from $\{0, 1\}$. Thus the Combinatorial Nullstellensatz tells us that upon expanding and simplifying Q, the coefficient appearing in front of the monomial $\eta_1 \eta_2 \cdot \ldots \cdot \eta_{2p-2}$ has to vanish and as this coefficient is

$$= 1 - (p-1)!^2 \mu(P_1, P_2, \dots, P_{2p-2})$$

the desired conclusion follows from WILSON'S Theorem. □

Remark 2.4. Given an arbitrary cloudy sequence, there are $2p-1$ possibilities to apply this lemma and the equations arising thereby will be referred to as the *conditional equations.* The argument just encountered can also be carried out in a one dimensional setting and there it directly yields an alternative proof of Fact 2 from the introduction. Thus one might hope for the two dimensional case that by combining and manipulating the conditional equations in a sufficiently clever way one could similarly prove ($\boxplus$). It can be shown, however, that there are some sequences which are not cloudy but nevertheless satisfy the conditional equations. Still, these counterexamples do by no means preclude the possibility of establishing property B by extracting certain polynomial equations from the Combinatorial Nullstellensatz and then proving that their solutions are only the desirable ones. They just indicate that to proceed along these lines one has to work somewhat more strategically and in fact to some extent this is what we shall do in the sequel.

Something the conditional equations do indeed imply is stated in

Corollary 2.5. *Any two linearly dependent points appearing in the same cloudy sequence are equal.*

Proof. Suppose that the sequence $(P_1, P_2, \dots, P_{2p-1})$ is cloudy and that $\alpha P_1 + \beta P_2 = 0$ for some $\alpha, \beta \in \mathbb{F}_p$ not vanishing simultaneously. The conditional equations associated with P_2 and P_1 read

$$\mu(P_1, P_3, \dots, P_{2p-1}) = 1 \qquad \text{and} \qquad \mu(P_2, P_3, \dots, P_{2p-1}) = 1.$$

Multiplying the first of them by α, the second one by β and adding up what results, we infer $\alpha + \beta = 0$ and from this $P_1 = P_2$ immediately follows. □

Somewhat unrelatedly, we have

Observation 2.6. *Every cloudy sequence containing $p-1$ pairwisely linearly dependent points is simple.*

Proof. By Fact 2 from the introduction or alternatively by Corollary 2.5 we know that the dependent points have to be equal. Now consider any cloudy sequence containing $p-1$ times e.g. the point $(1,0)$ and p further points (a_i, b_i) where $i = 1, 2, \dots, p$. Applying Fact 2 to the sequence $(b_1, b_2, \dots, b_{p-1})$ it follows that for some $k \in \mathbb{F}_p^\times$ we have $b_1 = b_2 = \ldots = b_{p-1} = k$ and in view of $(p-1) \cdot (1,0) + \sum\limits_{1 \leqslant i \leqslant p} (a_i, b_i) = (0,0)$ we finally obtain $b_p = k$. □

Example 2.7. As cloudy sequences cannot contain the origin, it follows from the last observation that 2 has property B. Slightly less trivially, there are eight points in $\mathbb{F}_3^2$ differing from the origin and these can be grouped together into four pairs of linearly dependent points.

Now as for $p = 3$ the length of cloudy sequences is five, it follows from the box–principle that any such sequence necessarily involves two linearly dependent points and thus we infer that 3 has property B as well. Having thereby seen that the two smallest cases can easily be dealt with separately, one should bear in mind that when we come to the more advanced aspects of our theory there will never arise any loss of generality by assuming $p \geqslant 5$ whenever this appears to be advantageous. Actually we shall reach a point later on (see Example 8.2) where we can easily dispose of the case $p = 5$ as well, whence for our most general argument, to be given in Proposition 10.1, it will be permissible to assume even $p \geqslant 7$.

Remark 2.8. Different proofs of Corollary 2.5 and Observation 2.6 may be found in [10], see Corollary 5.6.9 and Theorem 5.8.7 there.

3. A polynomial system of equations.

In this section, we shall occupy ourselves with a peculiar system of equations a sequence of points might satisfy and that does impose strong structural constraints. Throughout this preliminary investigation, we suppose to be working in an arbitrary field F whose characteristic is p and by points we shall mean elements of F^2.

Lemma 3.1. *Among any $2p-1$ points $P_1, P_2, \dots P_{2p-1}$ different from the origin and satisfying*

$$\mu(P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{2p-1}) = 0$$

for all $i \in [2p-1]$ there are $p+1$ pairwisely linearly dependent ones.

Proof. For brevity, we call a sequence of $2p-1$ points *magical* if it satisfies the hypothesis of the lemma. Clearly, this property is invariant under permutations. Now we claim

($*$) *If $(P_1, P_2, \dots, P_{2p-1})$ is a magical sequence such that for at most $p-1$ values of $i \in \{2, 3, \dots, 2p-1\}$ the points P_1 and P_i are linearly dependent, then for any point Q other than the origin the sequence $(Q, P_2, \dots, P_{2p-1})$ is also magical.*

To show this, we may assume that there is some $r \in [p]$ such that P_1 and P_i are linearly dependent if $i \leqslant r$ and linearly independent otherwise. If $m + k \leqslant 2p-1$ and $i_1, i_2, \dots, i_k$ are distinct elements of $[2p-1]$, we write $\mu^*_m(i_1, i_2, \dots, i_k)$ for the result of applying μ_m to the sequence remaining from $(P_1, P_2, \dots, P_{2p-1})$ after removing those of its terms whose indices are $i_1, i_2 \dots, i_k$. Finally, let $P_i = (a_i, b_i)$ for $i \in [2p-1]$ and $Q = (x, y)$. Now whenever $r < i \leqslant 2p-1$ we have $a_1 b_i - a_i b_1 \neq 0$ by our choice of r, moreover

$$\begin{aligned}(a_1 b_i - a_i b_1)\mu^*_{p-2}(1,i) &= b_i \left\{a_1 \mu^*_{p-2}(1,i) + b_1 \mu^*_{p-1}(1,i)\right\} - b_1 \left\{a_i \mu^*_{p-2}(1,i) + b_i \mu^*_{p-1}(1,i)\right\} \\ &= b_i \mu^*_{p-1}(i) - b_1 \mu^*_{p-1}(1) = 0,\end{aligned}$$

and similarly

$$\begin{aligned}(a_1b_i - a_ib_1)\mu^*_{p-1}(1,i) &= a_1\left\{a_i\mu^*_{p-2}(1,i) + b_i\mu^*_{p-1}(1,i)\right\} - a_i\left\{a_1\mu^*_{p-2}(1,i) + b_1\mu^*_{p-1}(1,i)\right\}\\ &= a_1\mu^*_{p-1}(1) - a_i\mu^*_{p-1}(i) = 0.\end{aligned}$$

Therefore $\mu^*_{p-2}(1,i) = \mu^*_{p-1}(1,i) = 0$, whence in particular

$$\mu(Q, P_2, \ldots, P_{i-1}, P_{i+1}, \ldots, P_{2p-1}) = x\mu^*_{p-2}(1,i) + y\mu^*_{p-1}(1,i) = 0.$$

This finishes the proof of $(*)$ in case $r = 1$, so we may suppose $r > 1$ from now on. Then there are some other equations we need to know and these require an additional idea: As P_1 is different from the origin, we may assume by symmetry that $a_1 \neq 0$. By linear dependency, this entails $a_2, \ldots, a_r \neq 0$. Now if $2 \leqslant i < j \leqslant r$, then $a_ib_j - a_jb_i = 0$ and thus

$$\begin{aligned}a_i\mu^*_{p-2}(1,i) - a_j\mu^*_{p-2}(1,j) &= a_i\{a_j\mu^*_{p-3}(1,i,j) + b_j\mu^*_{p-2}(1,i,j)\}\\ &\qquad - a_j\{a_i\mu^*_{p-3}(1,i,j) + b_i\mu^*_{p-2}(1,i,j)\}\\ &= (a_ib_j - a_jb_i)\mu^*_{p-2}(1,i,j) = 0,\end{aligned}$$

and similarly

$$\begin{aligned}a_i\mu^*_{p-1}(1,i) - a_j\mu^*_{p-1}(1,j) &= a_i\{a_j\mu^*_{p-2}(1,i,j) + b_j\mu^*_{p-1}(1,i,j)\}\\ &\qquad - a_j\{a_i\mu^*_{p-2}(1,i,j) + b_i\mu^*_{p-1}(1,i,j)\}\\ &= (a_ib_j - a_jb_i)\mu^*_{p-1}(1,i,j) = 0.\end{aligned}$$

In other words, we have

$$a_2\mu^*_{p-2}(1,2) = \ldots = a_r\mu^*_{p-2}(1,r)$$

as well as

$$a_2\mu^*_{p-1}(1,2) = \ldots = a_r\mu^*_{p-1}(1,r).$$

Using

$$a_2\mu^*_{p-2}(1,2) + \ldots + a_{2p-1}\mu^*_{p-2}(1,2p-1) = (p-1)\mu^*_{p-1}(1) = 0$$

and

$$a_2\mu^*_{p-1}(1,2) + \ldots + a_{2p-1}\mu^*_{p-1}(1,2p-1) = p\mu^*_p(1) = 0,$$

it follows from what we have shown by now that for any $i \in \{2, \ldots, r\}$ we have

$$(r-1)a_i\mu^*_{p-2}(1,i) = (r-1)a_i\mu^*_{p-1}(1,i) = 0,$$

whence by $(r-1)a_i \neq 0$ we arrive at

$$\mu^*_{p-2}(1,i) = \mu^*_{p-1}(1,i) = 0,$$

which in turn tells us

$$\mu(Q, P_2, \ldots, P_{i-1}, P_{i+1}, \ldots, P_{2p-1}) = x\mu^*_{p-2}(1,i) + y\mu^*_{p-1}(1,i) = 0$$

as before. Thereby, $(*)$ is proved.

Now assume that there was a magical sequence violating our lemma. Applying $(*)$ very often, we inferred that then the sequence whose first $p-1$ terms are $=(0,1)$ and whose remaining p terms are $=(1,0)$ was also magical, but clearly this is not the case. □

Remark 3.2. This easily implies ALON'S Permanent Conjecture for 2×2 matrices, cf. Conjecture 8.4 of [1].

It is worth our while to point out that the hypothesis of our lemma can still be weakened further.

Proposition 3.3. *Suppose that a sequence* $\mathsf{P} = (P_1, P_2, \ldots, P_{2p-1})$ *of points different from the origin, two further points* Q *and* R *also different from the origin and two disjoint subsets* A *and* B *of* $[2p-1]$ *the cardinality of whose union is less than* p *satisfy the following three conditions:*

(a) If $i \in A$*, then* Q *and* P_i *are linearly dependent.*
(b) If $i \in B$*, then* R *and* P_i *are linearly dependent.*
(c) If $i \in [2p-1] - (A \cup B)$*, then* $\mu(P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_{2p-1}) = 0$.

Then P *contains* $p+1$ *points that are pairwisely linearly dependent.*

Proof. It suffices to consider the case, where Q and R are linearly independent, for otherwise we may replace the quadruple (A, B, Q, R) by $(A \cup B, \emptyset, Q, X)$ for some appropriately selected point X. Applying some automorphism of F^2 to the whole situation if necessary, we may further suppose in view of Observation 2.2 that $Q = (1,0)$ and $R = (0,1)$. Now as usual let $P_i = (a_i, b_i)$ for all $i \in [2p-1]$ and we also continue to use μ^* as in the previous proof. Note that $b_i = 0$ whenever $i \in A$ and $a_i = 0$ whenever $i \in B$ by conditions (a) and (b), respectively. Hence for all $i \in A$ we have $a_i \neq 0$ by $P_i \neq 0$ and taking also (c) into account we infer $a_i \mu^*(i) = 0$ for all $i \in [2p-1] - A$. Moreover, if i and i' denote distinct members of A, then $a_i \mu^*(i) = a_i a_{i'} \mu^*(i, i') = a_{i'} \mu^*(i')$ and this tells us that for some $\alpha \in F$ we have $a_i \mu^*(i) = \alpha$ whenever $i \in A$. Finally we find

$$|A| \cdot \alpha = \sum_{i \in A} a_i \mu^*(i) = \sum_{i \in [2p-1]} a_i \mu^*(i) = p \mu_p(P_1, P_2, \ldots, P_{2p-1}) = 0,$$

whence $\mu^*(i) = 0$ for all $i \in A$. Similarly one verifies this equation for all $i \in B$ and taken together with (c) these facts reveal that our sequence P satisfies the hypothesis of Lemma 3.1, which in turn entails the desired conclusion. □

Corollary 3.4. *Suppose that* p *is odd, let* a*,* b *and* c *denote three elements of* F *that are not vanishing simultaneously and let* $\mathsf{P} = (P_1, P_2, \ldots, P_{2p-3})$ *a sequence of points different from* *the origin such that for all $i \in [2p-3]$ we have*

$$a\mu_{p-3}(P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{2p-3}) + 2b\mu_{p-2}(P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{2p-3}) \\ + c\mu_{p-1}(P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{2p-3}) = 0.$$

Then some $p-1$ terms from P *are pairwisely linearly dependent.*

Proof. As the conclusion of this statement is not affected by passing from the field F to an arbitrary extension, it is permissible to suppose that $b^2 - ac$ is a square in F and thus that there are points $P_{2p-2} = (r, s)$ and $P_{2p-1} = (u, v)$ different from the origin for which

$$ax^2 + 2bxy + cy^2 = (rx + sy)(ux + vy)$$

holds as an equation between polynomials. Now note that the sequence $(P_1, P_2, \dots, P_{2p-1})$ just constructed satisfies the hypothesis of Proposition 3.3 with $Q = P_{2p-2}$, $R = P_{2p-1}$, $A = \{2p-2\}$ and $B = \{2p-1\}$. □

4. The strategic equations.

For any points $A = (u, v)$ and $B = (x, y)$ from $\mathbb{F}_p^2$, we write $[AB] = uy - vx$. The reader is reminded of the equation

$$A[BC] + B[CA] + C[AB] = 0$$

valid for any three points $A, B, C \in \mathbb{F}_p^2$.

The following result, when applied in all possible ways to a given cloudy sequence, leads to a plethora of equations shedding so much light onto the whole problem that we are going to call them *strategic*.

Proposition 4.1. *Let $p > 2$ and suppose that a suspicious sequence $(A, B, C, P_1, \dots, P_{2p-5})$ is given. Then writing*

$$\mu^*(X, Y, Z) = \mu(X, Y, Z, P_1, \dots, P_{2p-5})$$

for all $X, Y, Z \in \mathbb{F}_p^2$, we have

$$[BC]\mu^*(A, A, A) + [CA]\mu^*(B, B, B) + [AB]\mu^*(C, C, C) \\ + 3\{[BC] + [CA] + [AB]\}\mu^*(A, B, C) = 0.$$

Proof. If two among the three points A, B and C are equal, then this formula is true even irrespective of the definition of μ^*, so we may assume additionally that these points are distinct and hence pairwise linearly independent. Exploiting Observation 2.2 we see that the validity of the strategic equations is not affected by applying automorphisms of $\mathbb{F}_p^2$ to the sequence under discussion and thus we may also suppose $A = (1, 0)$, $B = (0, 1)$ and $C = (x, y)$ for some $x, y \in \mathbb{F}_p$, where $xy \neq 0$. Our goal is then to prove

$$(x^3 - x)\mu^+_{p-4} + 3x(x-1)(y-1)\mu^+_{p-3} + 3(x-1)y(y-1)\mu^+_{p-2} + (y^3 - y)\mu^+_{p-1} = 0,$$

where we have written μ^+_m in place of $\mu_m(P_1, P_2, \ldots, P_{2p-5})$ for $m \in \{p-4, p-3, p-2, p-1\}$. Let $P_i = (u_i, v_i)$ for all $i \in [2p-5]$, take $2p-5$ variables $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2p-5}$ and set

$$U = \sum_{1 \leqslant i \leqslant 2p-5} u_i \varepsilon_i \qquad \text{as well as} \qquad V = \sum_{1 \leqslant i \leqslant 2p-5} v_i \varepsilon_i.$$

We now divide into three cases that are not mutually exclusive but cover all possibilities.

First Case: $x = 1$ *or* $y = 1$.

By symmetry we may suppose $x = 1$ and what remains to be shown is $(y^3 - y)\mu^+_{p-1} = 0$. This is clear if $y \in \{-1, 0, 1\}$, so from now on let this be not the case. Consider the polynomial

$$Q = \prod_{m \in \mathbb{F}_p - \{1\}} (U + m) \cdot \prod_{n \in \mathbb{F}_p - \{0,1,y,y+1\}} (V + n)$$

and assume that for some choice of $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2p-5} \in \{0, 1\}$ we had $Q \neq 0$. Then $U = -1$, $V \in \{0, -1, -y, -(y+1)\}$ and defining $I = \{i \in [2p-5] \mid \varepsilon_i = 1\}$ as well as

$J =$	$\{A\}$	$\{A, B\}$	$\{C\}$	$\{B, C\}$
if $V =$	0	-1	$-y$	$-(y+1)$

we find $\sum J + \sum\limits_{i \in I} P_i = 0$, contrary to the suspiciousness of $(A, B, C, P_1, \ldots, P_{2p-5})$.

It has thereby been shown that our assumption regarding the non–zeroes of Q must have been wrong and looking at the coefficient of $\varepsilon_1 \varepsilon_2 \cdot \ldots \cdot \varepsilon_{2p-5}$ one sees that this can only mean $\mu^+_{p-1} = 0$.

Second Case: $x = -1$ *or* $y = -1$.

As before, it suffices to consider the case $x = -1$ and this time we have to prove

$$(y-1)\{6\mu^+_{p-3} - 6y\mu^+_{p-2} + (y^2 + y)\mu^+_{p-1}\} = 0.$$

This is plain if $y = 1$, the case $y = 0$ has already been excluded at the beginning and $y = -1$ is also impossible for then we had $A + B + C = 0$. Therefore we may suppose $y \notin \{-1, 0, 1\}$ and setting

$$H'(\xi, \eta) = (y^2 + y)\xi^2 - 2y\xi\eta + 2\eta^2 + (y+1)(y\xi - 2\eta)$$

we find that the polynomial

$$Q' = \prod_{m \in \mathbb{F}_p - \{-1,0,1\}} (U + m) \cdot \prod_{n \in \mathbb{F}_p - \{0,1,y,y+1\}} (V + n) \cdot H'(-U, -V)$$

has total degree at most $2p-5$ and its coefficient belonging to $\varepsilon_1\varepsilon_2 \cdot \ldots \cdot \varepsilon_{2p-5}$ is

$$\begin{aligned}
&= (p-1)!(p-4)!(y^2+y)\mu^+_{p-1} - 2(p-2)!(p-3)!y\mu^+_{p-2} + 2(p-3)!(p-2)!\mu^+_{p-3} \\
&= -(p-2)!(p-4)!\{(y^2+y)\mu^+_{p-1} - 6y\mu^+_{p-2} + 6\mu^+_{p-3}\}.
\end{aligned}$$

Thus if our claim was wrong, then by the Combinatorial Nullstellensatz there existed values $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{2p-5} \in \{0,1\}$ for which $Q' \neq 0$. Then $U \in \{-1,0,1\}$ and $V \in \{0,-1,-y,-(y+1)\}$ but as

$$H'(1,y) = H'(1,y+1) = H'(0,0) = H'(0,y+1) = H'(-1,0) = H'(-1,1) = 0$$

there are on the whole only six possibilities left for the pair (U,V) and stipulating

$$I = \{i \in [2p-5] \mid \varepsilon_i = 1\}$$

as well as

$J =$	$\{A\}$	$\{A,B\}$	$\{B\}$	$\{A,C\}$	$\{C\}$	$\{B,C\}$
if $(U,V) =$	$(-1,0)$	$(-1,-1)$	$(0,-1)$	$(0,-y)$	$(1,-y)$	$(1,-y-1)$

we find $\sum J + \sum\limits_{i\in I} P_i = 0$, which contradicts the suspiciousness of $(A,B,C,P_1,\ldots,P_{2p-5})$. This finishes the discussion of the second case.

Third Case: $x \neq \pm 1$ *and* $y \neq \pm 1$.

Recalling that also $x \neq 0$ and $y \neq 0$ we can argue as before, using this time the polynomial

$$Q'' = \prod_{m\in\mathbb{F}_p-\{0,1,x,x+1\}} (U+m) \cdot \prod_{n\in\mathbb{F}_p-\{0,1,y,y+1\}} (V+n) \cdot H''(-U,-V),$$

where

$$\begin{aligned}
H''(\xi,\eta) = {} & (y^3-y)\xi(\xi-x)(\xi-x-1) \\
& + (x-1)(y-1)\xi\eta(y\xi + x\eta - 2xy - x - y) \\
& + (x^3-x)\eta(\eta-y)(\eta-y-1).
\end{aligned}$$

Noting that

$$\begin{aligned}
H''(0,0) &= H''(0,y) = H''(0,y+1) = H''(1,y) = H''(1,y+1) = H''(x,0) \\
&= H''(x,1) = H''(x+1,0) = H''(x+1,1) = H''(x+1,y+1) = 0,
\end{aligned}$$

we can replace the above table by defining

$J =$	$\{B\}$	$\{A\}$	$\{A,B\}$	$\{C\}$	$\{B,C\}$	$\{A,C\}$
for $(U,V) =$	$(0,-1)$	$(-1,0)$	$(-1,-1)$	$(-x,-y)$	$(-x,-y-1)$	$(-x-1,-y)$

and the rest carries over. □

5. Excluding three collinear points.

Now we come to the first substantial partial results towards (⊞) and to motivate them, suppose you are given some cloudy sequence and want to investigate it. As it certainly cannot contain p equal points, the box principle entails that at least three distinct points have to be present. Now if you already knew that the sequence under consideration was simple, then this told you that such three points could not form an arbitrary configuration: Rather, they either have to be collinear or together with the origin they have to be the vertices of some trapezoid. Let us call triples of distinct points falling under either of these two categories *clean* for the following lines. Now obviously it would be very useful if we devised some argument establishing that any triple of distinct points occurring in a cloudy sequence had to be clean, and in fact it could be shown that this statement then yielded property B by an elementary argument not relying on anything developed in sections 3 or 4. With some likelihood, however, the assertion we are speaking about is highly difficult to justify. So what we shall do instead in the following two sections is that we start with a cloudy sequence about which we already assume that it involves at least one clean triple and then prove the corresponding *reconstruction hypotheses* stating that the remaining $2p-4$ points have to attach to the three preselected ones in the expected way. The first of these is given by

Proposition 5.1. *Every cloudy sequence including three distinct but collinear points is simple.*

Proof. We may suppose $p \geqslant 5$. Take a cloudy sequence $(A, B, C, P_1, \dots, P_{2p-4})$ in which the three distinct points A, B and C are lying on a common line. By Corollary 2.5 this line cannot pass through the origin, so there are points X, Y satisfying $[XY] \neq 0$ together with three distinct numbers $a, b, c \in \mathbb{F}_p$ such that $A = X + aY$, $B = X + bY$ and $C = X + cY$. Setting

$$\mu_i^*(U, V, W) = \mu(U, V, W, P_1, \dots, P_{i-1}, P_{i+1}, \dots, P_{2p-4})$$

for any $U, V, W \in \mathbb{F}_p^2$ and $i \in [2p-4]$, the strategic equations tell us that

$$\begin{aligned}[BC]\mu_i^*(A, A, A) + [CA]\mu_i^*(B, B, B) + [AB]\mu_i^*(C, C, C)& \\ + 3\{[BC] + [CA] + [AB]\}\mu_i^*(A, B, C) &= 0\end{aligned}$$

holds for all $i \in [2p-4]$. Taking the trilinearity of μ_i^* into account, this simplifies to

$$[XY](a-b)(b-c)(c-a)\{3\mu_i^*(X, Y, Y) + (a+b+c)\mu_i^*(Y, Y, Y)\} = 0,$$

and writing $Z = 3X + (a+b+c)Y$ we obtain $\mu_i^*(Y, Y, Z) = 0$ for all $i \in [2p-4]$. Noting that $Z = A + B + C \neq 0$, we infer from Proposition 3.3 that some $p+1$ among the points

$$Y, Y, Z, P_1, \dots, P_{2p-4}$$

are pairwise linearly dependent. Therefore the sequence we started with certainly contains $p-1$ pairwise linearly dependent points and thus has to be simple in view of Observation 2.6. □

6. Excluding a trapezoid.

In this section, we intend to prove a similar result for constellations of three points that taken together with the origin form a trapezoid. This turns out to be somewhat easier if the trapezoid under consideration is not a parallelogram, so we commence with this case.

Lemma 6.1. *Cloudy sequences containing three distinct points forming together with the origin a trapezoid that is not a parallelogram are simple.*

Proof. Let $p \geqslant 5$ and take a cloudy sequence $(A, B, C, P_1, \dots, P_{2p-4})$ as described in the hypothesis of our lemma. We may suppose that $[AB] \neq 0$ and $C = B + rA$ for some $r \notin \{-1, 0, 1\}$. Using μ_i^* for $i = 1, 2, \dots, 2p-4$ in the same meaning as in the previous proof, the strategic equations this time tell us $[AB](r^3 - r)\mu_i^*(A, A, A)$=0 for all $i \in [2p-4]$. Hence Proposition 3.3 is applicable to the sequence $(A, A, A, P_1, \dots, P_{2p-4})$ and the argument may be completed as before. □

More generally, we claim

Proposition 6.2. *Every cloudy sequence involving three distinct points that taken together with the origin form a trapezoid is simple.*

Proof. In the light of the foregoing lemma, it suffices to treat cloudy sequences containing two distinct points A and B together with their sum $A + B$. If the sequence under consideration includes no point distinct from A, B and $A + B$, then it follows from the circumstance that the sum of all involved points has to vanish that A or B occurs at least $p-1$ times, whereby the sequence is in particular simple. Thus we may restrict our attention to cloudy sequences $(A, B, A + B, C, P_1, \dots, P_{2p-5})$ in which $[AB] \neq 0$ and $C \neq A, B, A + B$. Choosing $r, s \in \mathbb{F}_p$ such that $C = rA + sB$ and writing

$$\mu^*(X, Y, Z) = \mu(X, Y, Z, P_1, \dots, P_{2p-5})$$

for all $X, Y, Z \in \mathbb{F}_p^2$, the conditional equations with A, B, $A+B$ and C omitted tell us

$$\begin{aligned} r\mu^*(A,A,B) + (r+s)\mu^*(A,B,B) + s\mu^*(B,B,B) &= 1, \\ r\mu^*(A,A,A) + (r+s)\ \mu^*(A,A,B) + \qquad s\mu^*(A,B,B) &= 1, \\ r\mu^*(A,A,B) + \qquad s\mu^*(A,B,B) &= 1, \\ \text{as well as} \qquad \mu^*(A,A,B) + \qquad \mu^*(A,B,B) &= 1. \end{aligned}$$

Further we know

$$\begin{aligned} &(r^3-r)\mu^*(A,A,A) + 3r(r-1)(s-1)\mu^*(A,A,B) \\ &\qquad + 3(r-1)s(s-1)\mu^*(A,B,B) + (s^3-s)\mu^*(B,B,B) = 0 \end{aligned}$$

for strategical reasons. Multiplying the last five equations in this order by $1-s^2$, $1-r^2$, $(r-s)^2+3(r+s)-4$, $-(r+s)$, 1 and adding up what this yields, we deduce

$$-2(r-1)(s-1) = 0.$$

Therefore we have $r=1$ or $s=1$. If $r=1$, then the three distinct points A, $A+B$ and C are collinear and we may invoke Proposition 5.1 to conclude that the sequence we consider is indeed simple and if $s=1$, then using the triple $(B, A+B, C)$ we can argue similarly. □

7. Obtaining a fourth point.

In order to say something about a general cloudy sequences going beyond what we have proved so far, it appears advantageous to hypothesize it to involve at least four distinct points. Thus to prevent our whole investigation from inconclusiveness, it seems advisable to dispose at some point of those cases, that cannot be analyzed in this way and to work this out is the objective of the present section. This in turn is prepared by the following

Observation 7.1. *Suppose that A, B and C are three pairwise linearly independent points from $\mathbb{F}_p^2$ and that α, β and γ denote three non–negative integers, the sum of which equals $2p-2$. Then calculating in $\mathbb{F}_p$ we have*

$$[BC]^\alpha[CA]^\beta[AB]^\gamma\mu(\underbrace{A,\ldots,A}_{\alpha},\underbrace{B,\ldots,B}_{\beta},\underbrace{C,\ldots,C}_{\gamma}) = \alpha!\beta!\gamma!.$$

Proof. By symmetry, we may suppose $\alpha \geqslant \beta, \gamma$. Note that by Observation 2.2 and Fermat's Theorem it suffices to consider the case $A=(1,0)$, $B=(0,1)$ and $C=(x,y)$, where $xy \neq 0$. If $\alpha \geqslant p$, then both sides of the equation under discussion are easily seen to vanish and for this reason we shall suppose $\alpha, \beta, \gamma \leqslant p-1$ from now on. Thus we need to show

$$(-x)^\alpha(-y)^\beta\binom{\gamma}{p-1-\alpha}x^{p-1-\alpha}y^{p-1-\beta} = \alpha!\beta!\gamma!$$

and by FERMAT'S Theorem again, this is equivalent to

$$(-1)^{\alpha+\beta} = \alpha!(p-1-\alpha)! \cdot \beta!(p-1-\beta)!.$$

Using WILSON'S Theorem, one finds $\alpha!(p-1-\alpha)! = (-1)^{\alpha}(p-1)! = (-1)^{\alpha+1}$, similarly $\beta!(p-1-\beta)! = (-1)^{\beta+1}$, and the desired conclusion follows. □

Lemma 7.2. *Every cloudy sequence involving at most three distinct points is simple.*

Proof. Let p be odd and take a cloudy sequence P in which the three distinct points A, B and C occur with multiplicities α, β and γ respectively, where $\alpha+\beta+\gamma = 2p-1$. Clearly $\alpha, \beta, \gamma \leqslant p-1$ and if we have, e.g., $\alpha \leqslant 2$, then $\beta+\gamma \geqslant 2p-3$, hence $p-1 \in \{\beta, \gamma\}$ and the simplicity of P follows from Observation 2.6. Thus we may suppose $\alpha, \beta, \gamma \geqslant 3$. Writing $\mu(a, b, c)$ in place of

$$\mu(\underbrace{A, \dots, A}_{a}, \underbrace{B, \dots, B}_{b}, \underbrace{C, \dots, C}_{c})$$

whenever a, b and c denote some non–negative integers the sum of which equals $2p-2$, the strategic equation with (A, B, C) singled out and a further copy of C omitted discloses

$$[BC]\mu(\alpha+2, \beta-1, \gamma-2) + [CA]\mu(\alpha-1, \beta+2, \gamma-2) + [AB]\mu(\alpha-1, \beta-1, \gamma+1)$$
$$+ 3\{[BC]+[CA]+[AB]\}\mu(\alpha, \beta, \gamma-1) = 0.$$

Multiplying this by $[BC]^{\alpha+1}[CA]^{\beta+1}[AB]^{\gamma}$ and dividing thereafter by $(\alpha-1)!(\beta-1)!(\gamma-2)!$ we infer in view of Corollary 2.5 and Observation 7.1, that

$$[CA]^2[AB]^2\alpha(\alpha+1)(\alpha+2) + [BC]^2[AB]^2\beta(\beta+1)(\beta+2) + [BC]^2[CA]^2(\gamma-1)\gamma(\gamma+1)$$
$$+ 3[BC][CA][AB]\{[BC]+[CA]+[AB]\}\alpha\beta(\gamma-1) = 0.$$

Now recall $\alpha A + \beta B + \gamma C = [BC]A + [CA]B + [AB]C = 0$, from which it easily follows that for some $k \in \mathbb{F}_p^{\times}$ we have $[BC] = k\alpha$, $[CA] = k\beta$ and $[AB] = k\gamma$. Substituting this into the previous equation and dividing what we get by $k^4\alpha\beta\gamma$, we conclude

$$\beta\gamma(\alpha+1)(\alpha+2) + \alpha\gamma(\beta+1)(\beta+2) + \alpha\beta(\gamma-1)(\gamma+1) + 3(\alpha+\beta+\gamma)\alpha\beta(\gamma-1) = 0,$$

i.e.

$$2(\alpha+1)(\beta+1)(\gamma+1) + (4\alpha\beta\gamma - 3\alpha\beta - 2)(\alpha+\beta+\gamma+1) = 0.$$

But as in $\mathbb{F}_p$ we have $\alpha+\beta+\gamma+1 = 0$, this entails $p-1 \in \{\alpha, \beta, \gamma\}$ and by Observation 2.6 the simplicity of P follows. □

Remark 7.3. The previous Lemma also follows from one of the main results of [11], see Theorem 1 there. A slight generalization that demands considerably more work has recently been obtained in [3], see Theorem 1(4). The proof given above is, however, genuinely different from the more elementary approaches pursued in these two papers, and it has been included here in order to illustrate a certain point we wish to make, namely that the method we have developed is fully appropriate to handle all cases one might find oneself confronted with when thinking about property B.

8. Excluding two further configurations.

We now embark on a systematic study of cloudy sequences containing at least four distinct points. Intuitively, the presence of four points A, B, C and D is the more useful the more of the sums that can be formed by adding some of them are distinct. Two important possibilities for such sums to be equal are that either one of these points equals the sum of the three other ones, e.g. $D = A + B + C$, or that they form the vertices of some parallelogram, e.g. $A + C = B + D$. These two special cases, however, can be treated directly and to facilitate our later arguments we shall do so in the present section.

Proposition 8.1. *Cloudy sequences including four distinct points that either form the vertices of some parallelogram or that are such that one of them coincides with the sum of the three others are simple.*

Proof. Let p be odd and take a cloudy sequence $(A, B, C, D, P_1, \dots, P_{2p-5})$ in which A, B, C and D are distinct and $D = A + \eta B + C$ for some $\eta \in \mathbb{F}_p$ satisfying $\eta^2 = 1$. Following the proof of Proposition 6.2, we set

$$\mu^*(X, Y, Z) = \mu(X, Y, Z, P_1, \dots, P_{2p-5})$$

for all $X, Y, Z \in \mathbb{F}_p^2$. Write $C = xA + yB$ with $x, y \in \mathbb{F}_p$. The conditional equations with A, B, C and D removed read

$$x(x+1)\mu^*(A,A,B) + (2xy + \eta x + y)\mu^*(A,B,B) + y(y+\eta)\mu^*(B,B,B) = 1,$$

$$x(x+1)\mu^*(A,A,A) + (2xy + \eta x + y)\mu^*(A,A,B) + y(y+\eta)\mu^*(A,B,B) = 1,$$

$$(x+1)\mu^*(A,A,B) + (y+\eta)\mu^*(A,B,B) = 1,$$

as well as

$$x\mu^*(A,A,B) + y\mu^*(A,B,B) = 1$$

respectively. Multiplying them by $y - \eta$, $x - 1$, $\eta x + y$, $(3+\eta)(1-x) - 4y$ and adding up the results, we deduce

$$\begin{aligned}(x^3 - x)\mu^*(A,A,A) &+ 3x(x-1)(y-1)\mu^*(A,A,B) \\ &+ 3(x-1)y(y-1)\mu^*(A,B,B) + (y^3 - y)\mu^*(B,B,B) = 2(1 - x - y).\end{aligned}$$

Comparing this with the strategic equation, where the triple (A, B, C) is accentuated and D is omitted, we obtain

$$2(1 - x - y) = 0.$$

For this reason, the points A, B and C are collinear and an application of Proposition 5.1 concludes the argument. □

Example 8.2. Utilizing the theory developed so far, we can now give an extremely quick proof that 5 possesses property B. To see this, suppose that $(A, B, P_1, \ldots, P_7)$ was a cloudy sequence but not a simple one, where $A = (1, 0)$ and $B = (0, 1)$. We call a point distinct from A and B *excluded*, if it does not appear among $P_1, \ldots, P_7$ and *present* otherwise. Also, two points are said to be *incompatible*, if not both of them are present. By 2.5, 5.1 and 6.2 all points except for $(2, 2)$, $(3, 4)$, $(4, 3)$, $(4, 4)$ are excluded. Also, $(4, 4)$ is excluded as added together with A and B it sums up to zero. The three points that remain to be discussed are mutually incompatible by 5.1 and 8.1, hence at most one of them can be present and we get a contradiction by 7.2.

9. Conics, quartics and inferring general position.

In this section, we work over an arbitrary field K whose characteristic is different from 2 and what we are interested in are the various possibilities that there are for quadruples of distinct points from the affine plane K^2. The classification we describe is neither particularly natural nor hard to obtain; but it perfectly fits to the general argument yielding ($\boxplus$) that shall be given later.—

By a *conic section*, we mean the set Γ of solutions $(x, y) \in K^2$ of an equation looking like

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

for some $a, b, c, d, e, f \in K$. Note that according to this definition also K^2 itself is regarded as a conic section. If $a = b = c = 0$ is not the case, then Γ is called a *proper conic section.* We say that Γ *passes through a point* $P \in K^2$ if it contains P.

Observation 9.1. *If a proper conic section passes through seven distinct points of the form*

$$0, X, Y, Z, Y + Z, Z + X, X + Y,$$

then there is a line passing through the origin and at least two of the three points X, Y and Z.

Proof. Since the property of X, Y and Z we are talking about is evidently invariant under invertible linear transformations from K^2 to itself, there is no loss of generality in assuming $X = (1, 0)$ and $Y = (0, 1)$. Setting $Z = (r, s)$ we have to show that either $r = 0$ or $s = 0$. As the general equation of a conic section passing through 0, X, Y and $X + Y$ is given by

$a(x^2 - x) + c(y^2 - y) = 0$, there are $A, C \in K$ not vanishing simultaneously such that

$$\begin{aligned} & A(r^2 - r) + C(s^2 - s) = 0, \\ & A(r^2 + r) + C(s^2 - s) = 0, \\ \text{and} \qquad & A(r^2 - r) + C(s^2 + s) = 0. \end{aligned}$$

These equations entail $2Ar = 2Cs = 0$. So if $A \neq 0$, we simply have $r = 0$ and if $A = 0$, then $C \neq 0$ and hence $s = 0$. □

Lemma 9.2. *If A, B, C and D denote four distinct points from K^2, then at least one of the following seven alternatives occurs:*

(a) Some non–empty subsequence of (A, B, C, D) has sum zero.

(b) Two among them are linearly dependent.

(c) Some three of them are collinear.

(d) Some three of them form together with the origin the vertices of a trapezoid.

(e) One of them is equal to the sum of the three other ones.

(f) They are the vertices of some parallelogram.

(g) The fourteen sums that can be formed by taking one, two or three of them are distinct. Moreover, if these fourteen sums are grouped together into the seven pairs

$$(A, B + C + D), (B, A + C + D), (C, A + B + D), (D, A + B + C),$$
$$(A + B, C + D), (A + C, B + D) \text{ and } (A + D, B + C),$$

then it is neither possible to choose four of these pairs such that the eight points they contain are collinear nor is it possible to select six of these pairs for which the twelve points they consist of lie on a proper conic section.

Proof. We suppose that (g) is not valid and show that this yields one of the other six cases. There are three possibilities for (g) to fail and we will discuss them separately.

First, if the fourteen sums under consideration are not distinct, then either (a) is satisfied or, changing the names of A, B, C and D accordingly, one of the equations $A + B = C$, $A+B+C = D$ or $A+B = C+D$ must hold, which in turn means that (d), (e) or (f) occurs.

Second, suppose that the fourteen relevant sums are distinct but that some line g passes through eight of them coming from four of the pairs mentioned above. If g contains at least three of the points A, B, C and D, we are in case (c). If g involves exactly two of them, say A and B, then it also has to pass through $A + C$ or $B + C$ and in either of these cases (b) or (d) occurs. Finally, if g contains only one of our four points, then it necessarily passes through $A + B$, $A + C$ and $A + D$ and clearly this implies that B, C and D are collinear, i.e. that (c) holds.

Third, suppose again that the fourteen sums under discussion are distinct but that certain twelve of them coming from six of the relevant pairs are lying on a common proper conic section Γ. Then, upon relabeling A, B, C and D if required, we may suppose that Γ passes in particular through the points A, B, $A+C$, $B+C$, $A+D$, $B+D$ and $A+C+D$. Translating everything by $-A$, we see that the points $X=B-A$, $Y=C$ and $Z=D$ satisfy the hypothesis of Observation 10.1. Therefore there is some line h passing through A and at least two of the points B, $A+C$ and $A+D$. If h contains $A+C$ and $A+D$, then C and D satisfy (b) and if h contains, e.g., B and $A+C$, then either A and B are as in (b) or we get (d). □

For the application we have in mind possibility (g) is, of course, the most challenging one and the remainder of this section is directed towards reformulating it in a more perspicuous way, which requires some further concepts. By a *quartic curve* Σ, we mean the set of solutions $(x,y)\in K^2$ of an equation

$$ax^4+bx^3y+cx^2y^2+dxy^3+ey^4+P(x,y)=0,$$

where P denotes an arbitrary polynomial whose total degree is at most three. The vector (a,b,c,d,e) is referred to as the *leading quintuple* of Σ. Evidently, for every $M\subseteq K^2$ the set of leading quintuples of quartic curves passing through M forms a subvector space of K^5.

Definition 9.3. Four points $A,B,C,D\in K^2$ are said to be in general position if the fourteen sums that can be formed by adding one, two or three of them together are distinct and if moreover the space of leading quintuples of quartic curves passing through these fourteen sums is at most two dimensional.

It will be shown below that any four points as described in 9.2(g) are in general position and the verification of this is prepared by two further observations. The first of these is only going to be used for $n=5$ and $n=8$, but nevertheless we state it in full generality.

Observation 9.4. *Let $n\geqslant 5$ and suppose that $P_1,P_2,\dots,P_n$ are distinct points from K^2. Then either all but one of them are collinear or the subvector space of K^3 consisting of those triples (a,b,c) for which there are $d,e,f\in K$ such that the conic section defined by*

$$ax^2+bxy+cy^2+dx+ey+f=0$$

passes through all of these points has at most dimension one.

Proof. Otherwise let $n\geqslant 5$ be any integer for which this is false and take a sequence $P_1,P_2,\dots,P_n$ of points exemplifying this failure. Let $m\in\{2,3,\dots,n-2\}$ be the largest number of collinear points among them and upon renumbering the indices we may suppose that $P_1,\dots,P_m$ are lying on a common line.

First Case: $m \geqslant 3$.
As the assertion we seek to establish is invariant under translations and automorphisms of K^2, we may also suppose that writing $P_i = (r_i, s_i)$ for all $i \in [n]$ we have $s_1 = s_2 = \ldots = s_m = 0$. Consider an arbitrary equation $ax^2 + bxy + cy^2 + dx + ey + f = 0$ defining a conic section Γ passing through $P_1, P_2, \ldots, P_n$. Then there are at least three distinct values of x satisfying $ax^2 + dx + f = 0$, e.g. $x = r_1, r_2, r_3$, and thus we have $a = d = f = 0$. Hence the equation of Γ may be rewritten as $(bx + cy + e)y = 0$ and since $s_{m+1}, s_{m+2} \neq 0$ by our choice of m, it follows that $b(r_{m+1} - r_{m+2}) + c(s_{m+1} - s_{m+2}) = 0$. All this means that the second alternative mentioned in our claim occurs.

Second Case: $m = 2$.
For simplicity let $P_1 = (0, 0)$, $P_2 = (1, 0)$ and $P_3 = (0, 1)$. The equations of conic sections passing through these points look like $a(x^2 - x) + bxy + c(y^2 - y) = 0$ and as the space of possible values of (a, b, c) that can occur here has at least dimension two it follows that there are $A, B \in K$ not vanishing simultaneously such that P_4 and P_5 solve $A(x^2 - x) + Bxy = 0$. The latter equation may be rewritten as $(Ax + By - A)x = 0$ and thus its set of solutions is the union of two lines. Hence by the box principle some three among the points $P_1, \ldots, P_5$ have to be collinear, which, however, contradicts the maximality of m. □

In the following, a *quadratic surface* Ω is defined to be the set of solutions $(x, y, z) \in K^3$ of an equation such as

$$ax^2 + by^2 + cz^2 + dyz + ezx + fxy + gx + hy + iz + j = 0.$$

The vector (a, b, c, d, e, f) will be known as the *leading sextuple* of Ω.

Observation 9.5. *Suppose that $P_1, P_2, \ldots, P_7$ are seven distinct points from K^3 for which the space of leading sextuples of quadratic surfaces containing them is at least four dimensional. Then either four of these points are collinear or six are coplanar.*

Proof. Assume that the points $P_1, P_2, \ldots, P_7$ constituted a counterexample. For brevity, we call a quadratic surface *nice* if it passes through these points. Again the problem we are concerned with is invariant under translations and automorphisms of K^3, whence it always will be allowed to suppose that the four points $O = (0, 0, 0)$, $L' = (1, 0, 0)$, $L'' = (0, 1, 0)$ and $L''' = (0, 0, 1)$ occur among $P_1, \ldots, P_7$. Then the general form of an equation of a nice quadratic surface is given by

$$(\circledast) \qquad a(x^2 - x) + b(y^2 - y) + c(z^2 - z) + dyz + ezx + fxy = 0.$$

We commence by showing

$(*)$ *No five among the points $P_1, \ldots, P_7$ are coplanar.*

Otherwise, we may suppose $P_1 = O$, $P_2 = L''$, $P_3 = L'''$, $P_7 = L'$ and that the first coordinates of P_4 and P_5 vanish. Denoting the projection from K^3 onto K^2 given by $(x, y, z) \longmapsto (y, z)$ as π, we know that no four among the five distinct points $\pi P_1, \ldots, \pi P_5$ are collinear and hence by Observation 9.4 the space of triples (b, c, d) coming from nice surfaces as presented in $(\circledast)$ has at most dimension one. Thus also the surfaces defined by $x^2 - x = 0$, $xy = 0$ and $xz = 0$ are nice and as the point P_6 is different from L' it follows from this that its first coordinate vanishes as well. But this means that the six points $P_1, \ldots, P_6$ are coplanar and thereby $(*)$ is proved.

Next, we claim

$(**)$ *No three among the points $P_1, \ldots, P_7$ are collinear.*

For otherwise suppose that $P_1 = O$, $P_2 = L'$, $P_3 = u \cdot L'$ for some $u \in K - \{0, 1\}$, $P_6 = L''$ and $P_7 = L'''$. By the special form of P_3, all nice surfaces have $a = 0$. Thus the space of possibilities for (b, d, f) for which the surface defined by $(fx + b(y - 1) + dz) \cdot y = 0$ is nice has at least dimension two. Since the second coordinates of P_4 and P_5 cannot vanish by $(*)$, it follows from this that $P_4 - L''$ and $P_5 - L''$ are linearly dependent, i.e. that the line h containing P_4 and P_5 also passes through L''. Now, as the whole situation we consider is symmetric with respect to the second and third coordinate, a similar argument reveals that L''' likewise lies on h. Thus we have four collinear points, which proves $(**)$.

$(\boxtimes)$ *The quadruples (P_1, P_2, P_3, P_7), (P_1, P_2, P_4, P_6) and (P_1, P_3, P_4, P_5) cannot be coplanar at the same time.*

To verify this, we may suppose $P_1 = O$, $P_2 = L'$, $P_3 = L''$, $P_4 = L'''$, $P_5 = (0, r, s)$, $P_6 = (t, 0, u)$ and $P_7 = (v, w, 0)$ for some appropriate $r, s, t, u, v, w \in K$. By $(**)$, none of these six numbers can vanish. Take a nice surface Ω, whose equation is of the form $dyz + ezx + fxy = 0$, where, e.g., $d \neq 0$. Exploiting that Ω passes through P_5, we infer $rs = 0$ and this contradiction establishes $(\boxtimes)$.

With these remarks in mind, we can now start deriving the eventual contradiction. For this purpose, let $P_1 = O$, $P_2 = L'$, $P_3 = L''$ and $P_4 = L'''$. By $(**)$, there is a unique plane h containing P_5, P_6 as well as P_7 and by $(*)$ it is not possible for h to pass through two or more of the points L', L'' and L'''. So we may assume, e.g., that h contains neither L' nor L''. Take a proper nice surface of the form $(a(x - 1) + fy + ez) \cdot x = 0$. As the plane h does not pass through L', it cannot be determined by the equation $a(x - 1) + fy + ez = 0$ and hence the first coordinate of one among the points P_5, P_6 and P_7, say that of P_5, vanishes. Similarly, also the second coordinate of one of these points vanishes and since this cannot happen for P_5 again by $(**)$, we may suppose that it occurs for P_6. Now the quadruples (P_1, P_3, P_4, P_5) and (P_1, P_2, P_4, P_6) are coplanar, whence by $(\boxtimes)$ the third coordinate of P_7 has to be different from zero. Thus the above argument cannot be repeated once more, but it can only be obstructed by h passing through L'''. Thereby the quadruples (P_4, P_1, P_5, P_3), (P_4, P_1, P_6, P_2) and (P_4, P_5, P_6, P_7) have been discovered to be coplanar, which upon an obvious renumbering of indices contradicts ($\boxtimes$). This finally proves 9.5. □

Now we put these exercises to use by showing

Lemma 9.6. *Any four points as described in condition 9.2(g) are in general position.*

Proof. Otherwise assume (A, B, C, D) to be some counterexample. Setting

$$M = \tfrac{1}{2}(A + B + C + D),$$

the seven pairs listed above may be written as $M \pm P_1, \dots, M \pm P_7$ for some $P_1, \dots, P_7 \in K^2$. Let $P_i = (x_i, y_i)$ and $Q_i = (x_i^2, x_i y_i, y_i^2)$ for all $i \in [7]$. Clearly, the seven points $Q_1, \dots, Q_7$ from K^3 are distinct. Applying a translation of $-M$ to our assumption, there are three linearly independent vectors from K^5 that are leading quintuples of quartic curves passing through the fourteen points $\pm P_1, \dots, \pm P_7$. Let some such vectors be $(a_j, b_j, c_j, d_j, e_j)$, where $j = 1, 2, 3$. By symmetry with respect to the origin, there is for each $j \in [3]$ such a quartic curve defined by an equation looking like

$$a_j x^4 + b_j x^3 y + c_j x^2 y^2 + d_j x y^3 + e_j y^4 + f_j x^2 + g_j xy + h_j y^2 + i_j = 0.$$

These give rise to four quadratic surfaces passing through $Q_1, \dots, Q_7$, namely

$$a_j x^2 + b_j xy + c_j y^2 + d_j yz + e_j z^2 + f_j x + g_j y + h_j z + i_j = 0$$

for $j = 1, 2, 3$ as well as $y^2 - xz = 0$. As the leading sextuples of these surfaces are independent we arrive by Observation 9.5 at one of the following two possibilities.

First Case: Certain four among the points $Q_1, \dots, Q_7$ are collinear.

If this occurs, e.g., for Q_1, Q_2, Q_3 and Q_4, then the space of triples (a, b, c) for which some conic section of the form $ax^2 + bxy + cy^2 + d = 0$ passes through $\pm P_1$, $\pm P_2$, $\pm P_3$ and $\pm P_4$ has at least dimension two and thus by Observation 10.4 applied with $n = 8$ some seven of these eight points have to belong to a common line h. Plainly, h has to pass through the origin and hence contains all eight points under discussion, which contradicts the first additional clause of 10.2(g).

Second Case: Some six among the points $Q_1, \dots, Q_7$ are coplanar.

If this happens, e.g., for $Q_1, \dots, Q_6$, then the points $M \pm P_1, \dots, M \pm P_6$ lie on a common conic section, which is again contradictory. □

10. The general case.

Now let us have some fun.

Proposition 10.1. *Every cloudy sequence including four points in general position is simple.*

Proof. Let $p \geqslant 7$ and assume that some cloudy but not simple sequence

$$\mathsf{P} = (A, B, C, D, P_1, \dots, P_{2p-5})$$

in which the first four points mentioned are in general position existed. Note that $2p-5 > p$, whence at least two distinct points have to be present in $\mathsf{P}' = (P_1, \dots, P_{2p-5})$ and to facilitate a construction to be encountered below, we may suppose as usual that the points $E = (1, 0)$ and $F = (0, 1)$ occur there. By Definition 9.3, we know that the space V of leading quintuples of quartic curves passing through the fourteen sums $T_1, \dots, T_{14}$ that can be formed by adding one, two or three terms from the sequence (A, B, C, D) is at most two dimensional. Let $T_\ell = (r_\ell, s_\ell)$ for all $\ell \in [14]$. Evidently the subspace W of $\mathbb{F}_p^5$ consisting of all of all those vectors (a, b, c, d, e) that satisfy $au + bv + cx + dy + ez = 0$ for all $(u, v, x, y, z) \in V$ has at least dimension three. We now claim

(∗) *If $(\alpha_{40}, \alpha_{31}, \alpha_{22}, \alpha_{13}, \alpha_{04}) \in W$, then there are $\gamma_1, \dots, \gamma_{14} \in \mathbb{F}_p$ such that for all non–negative integers m, n with $m + n \leqslant 4$ we have*

$$\sum_{1 \leqslant \ell \leqslant 14} \gamma_\ell r_\ell^m s_\ell^n = \begin{cases} 0 & \text{if } m + n < 4, \\ \alpha_{mn} & \text{if } m + n = 4. \end{cases}$$

To see this, just apply the well–known principle from linear algebra stating that if $\mathsf{b}_1, \dots, \mathsf{b}_k, \mathsf{z}$ are some vectors from a common vector space U such that for all linear forms φ from the dual space of U with $\varphi(\mathsf{b}_1) = \ldots = \varphi(\mathsf{b}_k) = 0$ we also have $\varphi(\mathsf{z}) = 0$, then z can be written as a linear combination of $\mathsf{b}_1, \dots, \mathsf{b}_k$ to the case where $U = \mathbb{F}_p^{15}$, $k = 14$,

$$\mathsf{b}_\ell = (1, r_\ell, s_\ell, r_\ell^2, r_\ell s_\ell, s_\ell^2, r_\ell^3, r_\ell^2 s_\ell, r_\ell s_\ell^2, s_\ell^3, r_\ell^4, r_\ell^3 s_\ell, r_\ell^2 s_\ell^2, r_\ell s_\ell^3, s_\ell^4)$$

for $\ell = 1, \dots, 14$ and

$$\mathsf{z} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha_{40}, \alpha_{31}, \alpha_{22}, \alpha_{13}, \alpha_{04}).$$

Having thereby obtained (∗), we utilize it to establish

(∗∗) *If $(\alpha_{40}, \alpha_{31}, \alpha_{22}, \alpha_{13}, \alpha_{04}) \in W$ and $j \in [2p-5]$, then*

$$\alpha_{40}\mu^+_{p-5,j} + 4\alpha_{31}\mu^+_{p-4,j} + 6\alpha_{22}\mu^+_{p-3,j} + 4\alpha_{13}\mu^+_{p-2,j} + \alpha_{40}\mu^+_{p-1,j} = 0,$$

where $\mu^+_{k,j}$ serves as an abbreviation of $\mu_k(P_1, \dots, P_{j-1}, P_{j+1}, \dots, P_{2p-5})$ for $k \in \{p-5, p-4, p-3, p-2, p-1\}$.

Plainly, it suffices to verify this for $j = 2p-5$. Take $\gamma_1, \dots, \gamma_{14} \in \mathbb{F}_p$ as described in $(*)$ and form the polynomial

$$Q(x,y) = \sum_{1 \leqslant \ell \leqslant 14} \gamma_\ell \big((r_\ell + x)^{p-1} - 1\big)\big((s_\ell + y)^{p-1} - 1\big)$$

For non–negative integers m and n with $m+n \leqslant 4$ the coefficient accompanying $x^{p-1-m}y^{p-1-n}$ here is

$$\sum_{1 \leqslant \ell \leqslant 14} \gamma_\ell \binom{p-1}{m}\binom{p-1}{n} r_\ell^m r_\ell^n$$

and from this it follows that the total degree of Q is at most $2p-6$ and that the sum of its terms having this degree is

$$= \alpha_{40}x^{p-5}y^{p-1} + \alpha_{31}x^{p-4}y^{p-2} + \alpha_{22}x^{p-3}y^{p-3} + \alpha_{13}x^{p-2}y^{p-4} + \alpha_{04}x^{p-1}y^{p-5}$$

Now let $P_i = (g_i, h_i)$ for $i = 1, 2, \dots, 2p-6$, take $2p-6$ new variables $\varepsilon_1, \dots, \varepsilon_{2p-6}$, define

$$G = \sum_{1 \leqslant i \leqslant 2p-6} \varepsilon_i g_i, \qquad H = \sum_{1 \leqslant i \leqslant 2p-6} \varepsilon_i h_i$$

and view $Q(G,H)$ as a member of $\mathbb{F}_p[\varepsilon_1, \dots, \varepsilon_{2p-6}]$. As we have just seen, its total degree is at most $2p-6$ and the coefficient belonging to $\varepsilon_1\varepsilon_2 \cdot \ldots \cdot \varepsilon_{2p-6}$ is

$$= \sum_{m+n=4} (p-1-m)!(p-1-n)!\alpha_{mn}\mu^+_{p-1-m,2p-5},$$

i.e. $24(p-5)!^2$ times the expression we have claimed to vanish. Thus if $(**)$ failed, we could invoke the Combinatorial Nullstellensatz to obtain values $\varepsilon_1, \dots, \varepsilon_{2p-6} \in \{0,1\}$ for which $Q(G,H) \neq 0$. This then entailed the existence of some $\ell \in [14]$ such that

$$\gamma_\ell \big((r_\ell + G)^{p-1} - 1\big)\big((s_\ell + H)^{p-1} - 1\big) \neq 0$$

and hence $r_\ell + G = s_\ell + H = 0$. So defining $I = \{i \in [2p-6] \mid \varepsilon_i = 1\}$ we had $(r_\ell, s_\ell) + \sum_{i \in I} P_i = 0$, but obviously this contradicted the cloudiness of P. Thereby $(**)$ is proved.

Exploiting that W is at least three dimensional, we find some $(0, a, b, c, 0) \in W$ for which $a = b = c = 0$ is not the case and then $(**)$ yields

$$\begin{aligned} 2a\mu_{p-3}(E, F, P_1, \dots, P_{j-1}, &P_{j+1}, P_{2p-5}) + 3b\mu_{p-2}(E, F, P_1, \dots, P_{j-1}, P_{j+1}, P_{2p-5}) \\ &+ 2c\mu_{p-1}(E, F, P_1, \dots, P_{j-1}, P_{j+1}, P_{2p-5}) = 0 \end{aligned}$$

for all $j \in [2p-5]$. Recalling that E and F have been arranged to appear in the sequence P', we see that the hypothesis of Corollary 3.4 is satisfied. But in view of Observation 2.6, the only possibility for its conclusion to hold is that either E or F occurs with multiplicity $p-2$ in P'. It suffices to consider the former case and repeating the argument just given with some non–zero $(0, 0, a', b', c') \in W$ we discover that all of the remaining $p-3$ points from P'

are necessarily equal to F. Thereby P' has been entirely determined and the argument is not difficult to complete. For instance, for each $X \in \{A, B, C, D\}$ the equation $X + \eta E + \xi F = 0$ is insoluble with $\eta \in \{0, 1, \dots, p-2\}$ and $\xi \in \{0, 1, \dots, p-3\}$. Therefore, each of the points A, B, C and D has to belong to $K \cup L \cup M \cup N$, where

$$K = \mathbb{F}_p^\times \times \{0\}, \qquad L = \{0\} \times \mathbb{F}_p^\times, \qquad M = \{(y, 2) \in \mathbb{F}_p^2 \,|\, y \neq 0, 1\},$$
$$\text{and} \qquad N = \{(x, y) \in \mathbb{F}_p^2 \,|\, (x-1)(y-1) = 0 \text{ and } xy \neq 0\}.$$

But by 2.5, 2.6 and 6.2, K and N cannot contain any of these points and each of L and M can contain at most one of them. Thereby we have reached a contradiction. □

The following is easy by now.

Theorem 10.2. *Every prime number has property B.*

Proof. By our introductory remarks, it suffices to show that for all odd p every cloudy sequence P is simple. If P involves at most three distinct points, we may invoke Lemma 7.2, so from now on suppose that there are four distinct points A, B, C and D present in P. Applying Lemma 9.2 to these, we get seven possible cases, the first of which is, however, excluded by the cloudiness of P and the second of which cannot occur by Corollary 2.5. Also, if (c), (d), (e) or (f) occurs, the desired conclusion can be drawn from one of the Propositions 5.1, 6.2 or 8.1. Hence we may assume that (g) holds, but then A, B, C and D are in general position by Lemma 9.6 and Proposition 10.1 applies. □

11. Applications and Consequences.

Plenty of statements that have appeared in the literature roughly amount to saying that if the prime divisors of everything relevant have property B, then something interesting happens. Thus we are in the pleasing situation that it is fairly easy to deduce worth while corollaries from our main result, for the main work has already been done by others and all that remains to be done is cutting the redundant extra hypotheses from their existing theorems off. For the readers convenience, we conclude this paper with some examples illustrating that phenomenon.

1. Property C for prime numbers.

Continuing to use p to denote an arbitrary prime number, one can easily show by means of an argument that is similar to the one given for Fact 3 above that any sequence consisting of $3p-2$ points from $\mathbb{F}_p^2$ contains a subsequence the sum of whose terms vanishes and whose length is either p or $2p$. (For a slightly different proof of this see Corollary IIa of [13].) It follows by applying Fact 3 itself that every sequence of length $3p-2$ also possesses a non-empty zero–sum subsequence whose length is at most p. Thus one might wonder what those sequences of length $3p-3$ for which this conclusion is false look like and an old conjecture essentially due to van Emde Boas ([2]) asserts that if this occurs then the sequence under consideration necessarily consists of only three distinct points each of which appears with multiplicity $p-1$. The state of affairs that this is true for a particular value of p is usually expressed by saying that p has property C. As explained in Theorem 10.7 of [6], property B entails property C and thus we now know unconditionally: *Every prime number has property C.*

2. Property B for composite numbers.

Though the method of proof we have developed relies heavily on the field structure of $\mathbb{F}_p$, the result itself is a purely additive one and hence it makes sense to study similar questions with $\mathbb{F}_p^2$ replaced by $C_n \oplus C_n$, the direct sum of two cyclic groups of size n, where $n \geqslant 2$ denotes an arbitrary natural number. As the work of Kruyswijk and Olson reveals, Fact 3 itself carries over as follows: Every sequence consisting of $2n-1$ elements from $C_n \oplus C_n$ contains a non–empty subsequence whose sum equals 0. Defining the notions of suspicious and cloudy sequences in this context as expected, it has in analogy with ($\boxplus$) been conjectured that every cloudy sequence needs to contain some element with multiplicity $n-1$. If this holds, then n is said to have property B. Recently, W. Gao, A. Geroldinger and D. Grynkiewicz have obtained an extremely lengthy proof that n has property B provided that all its prime divisors do ([7]), which means that the combination of our results yields: *Every natural number has property B.*

It should be added that a complete classification of all cloudy sequences has, also quite recently, been carried out by W. Schmid in [14]. In fact, he is doing something more general there, namely he solves the analogous problem for arbitrary groups of rank two.

3. Property C for composite numbers.

A natural question that now presents itself asks to what extent the material mentioned in our first application generalizes to composite numbers. Since the earliest days of combinatorial zero–sum theory, it is known that every sequence of length $3n-2$ over $C_n \oplus C_n$ has a non–empty zero–sum subsequence which is short in the sense that its length is at most n. Also, n is said to have property C if every sequence of length $3n-3$ lacking short zero–sum subsequences consists of three distinct elements each of which occurs with multiplicity $n-1$. It has been established in [5] (see Theorem 3.2(2)), that property C is multiplicative, i.e. that if two natural numbers have property C, then so does their product. Hence we may conclude: *Every natural number has property C.*

4. van Emde Boas' *ν–invariant.*

With some applications to the determination of the Davenport constant of more complicated groups in mind, van Emde Boas defined $\nu(C_n \oplus C_n)$ to be the least number ν for which the following is true: If a sequence P containing at least ν elements from $C_n \oplus C_n$ has no non–empty subsequence whose sum is zero, then there is a coset of some proper subgroup of $C_n \oplus C_n$ containing all those members of that group which are not expressible as the sum of a possibly empty subsequence of P. It has been known that $\nu(C_n \oplus C_n) \in \{2n-2, 2n-1\}$ and that the smaller of these two values is the correct one if n has property C, see Section 5 of [2].

Fourth Conclusion: *For every $n \geqslant 2$ one has $\nu(C_n \oplus C_n) = 2n-2$.*

5. More Davenport constants.

In general, the Davenport constant $\mathsf{D}(G)$ of a finite Abelian group G is defined to be the least natural number d for which every sequence consisting of d elements from G contains a non–empty subsequence the sum of whose elements vanishes. The argument usually used to establish Fact 1 from the introduction can straightforwardly be modified to show that such a number always exists and that $\mathsf{D}(G) \leqslant |G|$. The widest classes of groups whose Davenport constants are currently known are cyclic groups, groups of rank two and p–groups, whereas for the general case there is at the moment not even a plausible conjecture. Quite frequently, when one intends to determine the Davenport constant of some group G not covered by the cases already mentioned, one finds oneself projecting the whole situation onto a quotient group of G and typically the more additional properties of that group are known the better the chances for success are. For instance, it has recently been shown by G. Bhowmik, I. Halupczok and J.–C. Schlage–Puchta [4] that if n is coprime to 6 and has property B, then $\mathsf{D}(C_3 \oplus C_{3n} \oplus C_{3n}) = 6n+1$. So if the reader has ever asked himself what $\mathsf{D}(C_3 \oplus C_{1005}^2)$ might be, he can now be assured that it indeed equals 2011. It seems conceivable that similar applications will emerge in the near future.

Acknowledgement I would heartily like to thank my advisor Dieter Gronau and Konrad Engel for arranging that I could obtain an academic position at the University of Rostock. Further thanks go to Alfred Geroldinger and Wolfgang Schmid who invited me to present the proof developed here at the University of Graz and for considerable help with the existing literature.

References

[1] BibliographyNoga Alon, ‘Combinatorial Nullstellensatz’, *Combinatorics, Probability and Computing* **8** (1999), 7–29.

[2] BibliographyP. van Emde Boas, ‘A combinatorial problem on finite Abelian groups II’, *Report ZW–1969–007, Stichting Mathematisch Centrum, Amsterdam 1969.*

[3] BibliographyGautami Bhowmik, Immanuel Halupczok and Jan–Christoph Schlage–Puchta, ‘The structure of maximal zero–sum free sequences’, *Acta Arithmetica* **143** (2010), 21–50.

[4] BibliographyGautami Bhowmik, Immanuel Halupczok and Jan–Christoph Schlage–Puchta, ‘Inductive methods and zero–sum free sequences’, *Integers* **9** *(2009), 515–536.*

[5] BibliographyWeidong Gao, Alfred Geroldinger and Wolfgang Schmid, ‘Inverse zero–sum problems’, *Acta Arithmetica* **128** (2007), 245–279.

[6] BibliographyWeidong Gao and Alfred Geroldinger, ‘On long minimal zero sequences in finite abelian groups’, *Periodica Mathematica Hungarica* **38** (1999), 179–211.

[7] BibliographyWeidong Gao, Alfred Geroldinger and David Grynkiewicz, ‘Inverse zero–sum problems III’, *Acta Arithmetica* **141** (2010), 103–152.

[8] BibliographyCarl Friedrich Gauß, ‘Disquistiones Arithmeticae’, Lipsiae in commissis apud Gerh. Fleischer Jun. 1801.

[9] BibliographyCarl Friedrich Gauß, ‘Theoria residuorum biquadraticorum. Commentatio Prima’, *Commentationes societatis regiae scientarum Gottingensis recentiores* **16** (1825); reprinted in Werke II, 65–92.

[10] BibliographyAlfred Geroldinger and Franz Halter–Koch, ‘Non–unique Factorization. Algebraic, Combinatorial and Analytic Theory’, *Pure and Applied mathematics, vol. 278, Chapman & Hall/CRC, 2006.*

[11] BibliographyGünter Lettl and Wolfgang Schmid, ‘Minimal zero–sum sequences in $C_n \oplus C_n$’, *European Journal of Combinatorics* **28** (2007), 742–753.

[12] BibliographyJohn E. Olson, ‘A combinatorial problem on finite Abelian groups’, *Journal of Number Theory* **1** (1969), 8–10.

[13] BibliographyChristian Reiher, ‘On Kemnitz’ Conjecture concerning lattice points in the plane’, *Ramanujan Journal* **13** (2007), 333–337.

[14] BibliographyWolfgang Schmid, ‘Inverse zero–sum problems II’, *Acta Arithmetica* **143** (2010) 333–343.

Institut für Mathematik, Universität Rostock, 18051 Rostock, Germany
E-mail address: `Christian.Reiher@uni-rostock.de`