A REMOVAL LEMMA FOR SYSTEMS OF LINEAR EQUATIONS OVER FINITE FIELDS

DANIEL KRÁL', ORIOL SERRA, AND LLUÍS VENA

Abstract. We prove a removal lemma for systems of linear equations over finite fields: let $X_1, \ldots, X_m$ be subsets of the finite field $\mathbb{F}_q$ and let A be a $(k \times m)$ matrix with coefficients in $\mathbb{F}_q$; if the linear system $Ax = b$ has $o(q^{m-k})$ solutions with $x_i \in X_i$, then we can eliminate all these solutions by deleting $o(q)$ elements from each X_i. This extends a result of Green [Geometric and Functional Analysis 15(2) (2005), 340–376] for a single linear equation in abelian groups to systems of linear equations. In particular, we also obtain an analogous result for systems of equations over integers, a result conjectured by Green. Our proof uses the colored version of the hypergraph Removal Lemma.

1. Introduction

In 2005, Green [6, Theorem 1.5] proved the so-called Removal Lemma for abelian groups. It roughly says that if a linear equation over an abelian group has not many solutions then one can delete all the solutions by removing few elements. This Removal Lemma for groups has its roots in the well–known Triangle Removal Lemma of Ruzsa and Szemerédi [13] (see also [3] and [10] for generalizations and applications of this important result in combinatorics) which says that if a graph with n vertices has only $o(n^3)$ triangles, then it can be made triangle–free by removing only $o(n^2)$ edges.

In [7], the authors gave a purely combinatorial proof, by using the Removal Lemma for graphs, of Green's algebraic version of the Removal Lemma for linear equations. This allows an extension of the result to non-abelian groups. In the same paper, the authors considered some extensions of the result to systems of equations in abelian and non–abelian groups which could be proved along the same lines. However to extend the result to general linear systems, the graph representation used in the mentioned paper presented serious limitations. Instead, the extensions to hypergraphs of the removal lemma, which have been recently proved by Nagle, Rödl, Schacht [11], Gowers [5] or Tao [18], seem to be the natural tool to achieve this goal.

Our main result is the following:

Theorem 1 (Removal Lemma for systems of equations)**.** *For all positive integers k and m, $k \leq m$, and every $\varepsilon > 0$, there exists $\delta > 0$ such that the following holds: Let $F = \mathbb{F}_q$ be the finite field of order q and $X_1, \ldots, X_m$ be subsets of F, let A be a $(k \times m)$ matrix with coefficients in F and let b be a vector in F^k.*

2000 *Mathematics Subject Classification.* 11B75.

Key words and phrases. Removal Lemma, Szemerédi Theorem.

Supported as project 1M0545 by Czech Ministry of Education.

Supported by the Catalan Research Council under project 2005SGR0258.

Supported by the Spanish Research Council under project MTM2005-08990-C01-C02.

If there are at most δq^{m-k} solutions of the system $Ax = b$, $x = (x_1, \ldots, x_m)$, with $x_i \in X_i$, then there exist sets $X'_1, \ldots, X'_m$ with $X'_i \subseteq X_i$ and $|X_i \setminus X'_i| \leq \varepsilon q$ such that there is no solution of the system $Ax = b$ with $x_i \in X'_i$.

Using the little o-notation, Theorem 1 asserts that if there are $o(q^{m-k})$ solutions of the system $Ax = b$ with $x_i \in X_i$, then there exist sets $X'_i \subseteq X_i$ such that $|X_i \setminus X'_i| = o(q)$ and there is no solution of the system $Ax = b$ with $x_i \in X'_i$. Throughout the paper, we will use more precise formulations without the little o-notation, but we occasionally use this notation if no confusion can arise.

By a standard argument Theorem 1 implies an analogous result in the integers. In particular it provides a proof of the following result conjectured by Green [6, Conjecture 9.4]:

Theorem 2. *Let k and m be integers with $k \leq m$ and let A be an integer $k \times m$ matrix of rank k. For every $\varepsilon > 0$, there exists $\delta > 0$ with the following property. Let $X \subseteq [N]$, and suppose that there are at most δN^{m-k} vectors x in X^m for which $Ax = 0$. Then $X = B \cup C$, such that there are no solutions of the system $Ax = 0$ with $x \in B^m$ and $|C| \leq \varepsilon N$.*

Proof. Let $c(A)$ be twice the sum of the absolute values of the coefficients in A plus 1. Let p be a prime such that $c(A) \cdot N \leq p \leq 2c(A) \cdot N$.

By the choice of p, there is a natural bijective correspondence between the solutions of the linear system $Ax = 0$ in $\mathbb{F}_p$ with $x \in X^m$ and the ones in the integers.

We apply Theorem 1 with $F = \mathbb{F}_p$ and $X_i = X$ for all i to obtain the result. □

A natural application of Theorem 2, which indeed motivated the extension of the removal lemma to hypergraphs, is the proof of the celebrated Theorem of Szemerédi on the existence of k–term arithmetic progressions in sets of integers with positive density. Actually Theorem 2 proves the strengthening by Varnavides [19] that a set of integers in $[1, n]$ with positive density contains $\Omega(n^2)$ arithmetic progressions of length k. This is so because the linear system which defines a k–term arithmetic progression in a set X has $|X|$ trivial solutions (corresponding to constant k–term progressions) which can only be removed by deleting all elements in X. Theorem 1 provides the analogous statement in the finite field context.

Corollary 3. *For every positive integer k and every $\varepsilon > 0$, there exists $\delta > 0$ such that if a subset X of the elements of the q-element field $\mathbb{F}_q$ contains at most δq^2 arithmetic progressions of length k, then the set X has at most εq elements.*

Corollary 3 above can also be proved by using the construction from Frankl and Rödl [4] and the hypergraph removal lemma (see [12]).

Our proof of Theorem 1 follows the main idea of the one presented in [7]. When the system is reduced to one equation our construction coincides with the one in that paper, thus it can be viewed as its natural generalization. As we have already mentioned, we use the edge-colored version of the hypergraph Removal Lemma, see Theorem 4 in Section 2, which follows from a more general result of Austin and Tao [1, Theorem 2.1].

Independently of us, Conjecture 9.4 from [6] was proved by Shapira [14] (see also [15]) whose method also yields a different proof of Theorem 1. Shapira's proof also reduces the problem to finding an appropriate representation of the system by a hypergraph in which one can identify certain subgraphs with solutions, and uses the colored version of the hypergraph Removal Lemma (Theorem 4) as our proof does.

However, his proof involves $O(m^2)$–uniform hypergraphs where our proof involves $(k+1)$–uniform hypegraphs. The two proofs follow a common approach but they differ in the particular ideas used to represent systems by hypergraphs.

We note that Theorem 1 might also be derived from the main result in Szegedy [17]. There the author proves a Symmetry Removal Lemma and describes a framework to apply it to Cayley Hypergraphs. Theorem 1 would follow from the Symmetry Removal Lemma once the conditions of validity within this setting are properly verified.

Let us also mention that the conclusion of Theorem 1 can be proven in a substantially easier way if we assume that every k columns of the matrix are linearly independent; we have reported on this result in [8]. Candela [2] has proved, independently of us, this result too.

2. The hypergraph Removal Lemma and outline of the proof

Let us recall some definitions on hypergraphs. A k–uniform hypergraph K is a collection $E = E(K)$ of k–subsets, called edges of K, of a ground set $V = V(K)$. An *edge–coloring* of K with r colors is a map $c : E(K) \to \{1, 2, \dots, r\}$. The hypergraph K is said to be t-partite if there is a partition of V in t parts and every edge in E intersects each part in at most one vertex.

Let H and K be two r–edge colored k–uniform hypergraphs. We say that K contains a copy of H if there is an injective homomorphism f from H to K, that is, there is an injective map $f : V(H) \to V(K)$ which preserves edges and their colors. Two such maps f, f' are equivalent if there is an automorphism g of H such that $f'(H) = fg(H)$ and the number of copies of H in K is the number of equivalence classes of maps. Two copies of H in K are said to be edge disjoint if so are the images of the corresponding maps. We say that K is H–free if there is no copy of H in K.

Our main tool for the proof of Theorem 1 is the following version of the hypergraph Removal Lemma which follows from a more general result of Austin and Tao [1, Theorem 2.1].

Theorem 4 (Austin and Tao [1])**.** *Let H be an edge-colored $(k+1)$-uniform hypergraph with m vertices. For every $\varepsilon > 0$ there exists $\delta > 0$ with the following property.*

Let K be an edge colored $(k+1)$-uniform hypergraph with M vertices. If the number of copies of H in K (preserving the colors of the edges) is at most δM^m, then there is a set $E' \subseteq E(K)$ of size at most εM^{k+1} such that the hypergraph K' with edge set $E(K) \setminus E'$ is H–free.

The general idea of the proof is to associate to the linear system $Ax = b$, where A has size $k \times m$, a pair of edge-colored $(k+1)$-uniform hypergraphs H and K. The hypergraph H has m edges and m vertices, and K is an m-partite hypergraph with mq vertices. The edges of H and of K are defined in such a way that there is a correspondence between copies of H in K and solutions of the linear system in $X_1 \times \cdots \times X_m$. More precisely, each solution gives rise to exactly q^k edge disjoint copies of H in K.

The bound on the number of solutions of our linear system translates to the fact that K contains $o(q^m)$ copies of H. At this point we apply the Removal Lemma for hypergraphs, Theorem 4, to find a set E' of edges with size $o(q^{k+1})$, such that, by removing E' from K we delete all copies of H.

Since the q^k copies of H corresponding to the same solution are edge–disjoint, a pigeonhole argument allows us to find $o(q)$ elements from each set X_i whose removal eliminates all the solutions of the system of equations.

3. Reductions of the system

The key point in our argument is the construction of the auxiliary hypergraphs H and K. Before we explain the details of this construction, we show that we can assume some properties of the given linear system $Ax = b$. In what follows, M^i denotes the i–th column of a matrix M and M_j denotes its j–th row.

Lemma 5. *Theorem 1 holds if it can be proved under the following assumptions.*

(i) *The matrix A has the form $A = (I_k|B)$ where I_k is the identity matrix.*
(ii) $b = 0$.
(iii) $m \geq k + 2$.
(iv) *Every two rows of B are linearly independent.*
(v) *Each row of B has at least two non-zero entries.*
(vi) *No column of A is the zero vector.*

Proof. We will establish these properties sequentially and assume the previous ones at each step.

(i) Observe that, by the nature of the statement of Theorem 1, there is no loss of generality in assuming that the matrix A has full rank k. Indeed, choose δ to be the minimum $\delta_{k'}$, $k' = 1, \ldots, k$, where $\delta_{k'}$ is the constant for full rank $k' \times m$ matrices. Consider a $k \times m$ matrix A. If the rank k' of the matrix A is smaller than k but the rank of the matrix $(A|b)$ is $k' + 1$, then there is no solution of the system $Ax = b$ at all and there is nothing to prove. Otherwise, let A' be a full-rank $k' \times m$ submatrix A' and b' the subvector b with entries corresponding to the rows of A'. Observe that if the system $Ax = b$ has at most δq^{m-k} solutions, then the system $A'x = b'$ has at most $\delta_{k'} q^{m-k'}$ solutions and the statement follows.

By an appropriate choice of basis, the matrix A can be assumed to be of the form $A = (I_k|B)$, where I_k denotes the $k \times k$ identity matrix.

(ii) If A is written in the form $(I_k|B)$, then the general statement of Theorem 1 follows by applying it to the system $Ax = 0$ once we replace the given first k sets $X_1, \ldots, X_k$ by $X_1 - b_1, \cdots, X_k - b_k$, where $b = (b_1, \ldots, b_k)$ (and leave the remaining sets $X_{k+1}, \ldots, X_m$ unchanged.)

(iii) Note that if $m = k + 1$ then Theorem 1 trivially holds with $\delta = \varepsilon$. Indeed, for each element $a \in X_{k+1}$ there is at most one solution to the system $Ax = 0$ with last coordinate a; since the number of solutions is at most δq, there must be at most $\varepsilon q = \delta q$ elements in X_{k+1} which belong to a solution of $Ax = 0$ with $x \in X_1 \times \cdots \times X_{k+1}$; by deleting these elements from X_{k+1}, we delete all the solutions. Thus, we can assume that $m \geq k + 2$.

(iv) Suppose on the contrary that rows B_i and B_j of B are not linearly independent, say $B_i = \lambda B_j$. This implies that every solution of the system $Ax = 0$ satisfies $x_i = \lambda x_j$. Therefore we can replace X_i by $X_i \cap (\lambda \cdot X_j)$, delete the j-th equation together with the j-th variable, and apply our theorem in the resulting setting: the obtained system contains one less equation and one less variable.

(v) We may assume that any row B_i of B has at least two non-zero entries. Otherwise the i–th equation would read $x_i + b_{i,j}x_j = 0$ for some $j \in [k+1, \dots, m]$. As in the preceding paragraph, we can replace the set X_j by $X_j \cap \left(-b_{i,j}^{-1} \cdot X_i\right)$ and consider the system obtained by eliminating the i-th equation and the i-th variable.

(vi) Suppose that A has a zero column, say $A^m = 0$. Set δ to be $\varepsilon\delta'$ where δ' obtained for $k' = k$ and $m' = m - 1$. If the set X_m contains at most εq elements, we can delete all elements of the set X_m and no solution of the system is left. Otherwise, if the system $Ax = b$ has at most δq^{m-k} solutions, then the system $A'x' = b$, where A' is the matrix obtained from A by deleting the m-th column, has at most $\delta q^{m-k}/(\varepsilon q) = \delta' q^{m-1-k}$ solutions and we can apply the statement for $m' = m - 1$ and $k' = k$.

□

4. Hypergraph representation and proof of Theorem 1

Let $Ax = 0$ be a linear system, where A is a $k \times m$ matrix with entries in F satisfying the properties (i)–(vi) of Lemma 5. For the hypergraph representation of the system $Ax = 0$ we shall use an auxiliary matrix associated to the matrix A which is described in Lemma 6 below. The support of a vector $x \in F^n$, denoted by $s(x)$, is the set of coordinates with a nonzero entry.

Lemma 6. *Let $A = (I_k|B)$ be a $(k \times m)$-matrix with coefficients in $\mathbb{F}_q$ satisfying the properties (i)–(vi) of Lemma 5. There are an $(m \times m)$ matrix C and m pairwise distinct $(k+1)$-subsets $S_1, \dots, S_m \subseteq [1, m]$ with the following properties:*

(1) *$AC = 0$*
(2) *$rank(C) = m - k$ (maximal under the first condition).*

Moreover, there is an ordering of the columns of B such that

(3) *For every i, $s(C_i) \subseteq S_i$ and $i \in s(C_i)$.*
(4) *For every i, there exists a subset $S_i' \subseteq S_i$ with $|S_i'| = k$ and $S_i \setminus S_i' \subseteq s(C_i)$ such that the set of columns $\{C^j,\ j \in [1, \dots, m] \setminus S_i'\}$ has rank $m - k$.*

The proof of Lemma 6 is postponed to Section 5. We now proceed to define a suitable hypergraph representation of the linear system which leads to a proof of Theorem 1.

Let C be the matrix associated to A and $S_1, \dots, S_m$ be the $(k+1)$–subsets of $[1, m]$ satisfying the properties stated in Lemma 6.

The hypergraph H is the $(k+1)$–uniform edge–colored hypergraph with vertex set $\{1, 2, \dots, m\}$ and with edges $S_1, S_2, \dots, S_m$, where the edge S_i is colored i.

The hypergraph K is the $(k+1)$–uniform m–partite edge–colored hypergraph with vertex set $\mathbb{F}_q \times [1, m]$ and with the following edge set. For every $u \in X_i$, K contains an edge $\{(a_j, j),\ a_j \in \mathbb{F}_q, j \in S_i\}$ if and only if

$$\sum_{j \in S_i} C_{ij} a_j = u,$$

and this edge is colored by i and labeled by u. Since the support $s(C_i)$ is nonempty and $|S_i| = k + 1$, K contains precisely q^k edges colored by i and labeled by x for each $x \in X_i$.

We next show that the hypergraphs K and H have the needed properties for the proof.

Claim 1. *If H' is a copy of H in K, then $x = (x_1, \ldots, x_m)$ is a solution of the system, where x_i is the label of the edge colored by i in H'.*

Proof. Since H' is a copy of H, it has m vertices and an edge of each color. By Lemma 6 (3) we have $i \in S_i$ for each i which implies $\cup_{i=1}^{m} S_i = [1, m]$. Hence the vertex set of H' is of the form $\{(a_1, 1), (a_2, 2), \ldots, (a_m, m)\}$. By the construction of K, it holds that $Ca = x$ where $a = (a_1, a_2, \ldots, a_m)$. Hence, $0 = ACa = Ax$ and x is a solution of the system. □

Claim 2. *For any solution $x = (x_1, \ldots, x_m)$ of the system $Ax = 0$ with $x_i \in X_i$, there are precisely q^k edge–disjoint copies of the edge–colored hypergraph H in the hypergraph K.*

Proof. Fix a solution $x = (x_1, \ldots, x_m)$ of $Ax = 0$ with $x_i \in X_i$, $1 \leq i \leq m$. First, we will show that there is a copy of H in K in which the edge colored i has label x_i, $1 \leq i \leq m$.

Since the matrix C has rank $m - k$ and satisfies $AC = 0$, the columns in C span the solution space in F^m and thus there is a vector $u = (u_1, \ldots, u_m)$ with $x = Cu$. In particular,

$$x_i =< C_i, u >= \sum_{j=1}^{m} C_{ij} u_j = \sum_{j \in S_i} C_{ij} u_j,$$

where the second equality follows from Lemma 6 (3). Therefore, for every i, the set $\{(u_j, j), j \in S_i\}$ is an edge of K colored i and labeled x_i. It follows that the edges $\{(u_j, j), j \in S_i\}$, $i = 1, \ldots m$, span a copy of H in K.

Since the kernel of C is k-dimensional, there are q^k vectors u satisfying $x = Cu$, and each of them corresponds to a copy of H in K. We next verify that these q^k copies are edge–disjoint.

Let $e = \{(a_j, j), j \in S_i\}$ be an edge of K colored by i and labeled $x_i \in X_i$. We show that all the q^k copies of H in K contain different edges colored by i and labeled x_i for each i. By Lemma 6 (4), there is a subset $S_i' \subseteq S_i$ of size k such that $\{C^j, j \notin S_i'\}$ is a set of $m - k$ linearly independent solutions of the system $Ax = 0$. Hence, we may find a vector $u = (u_1, \ldots, u_m)$ with $x = Cu$ such that $u_j = a_j$ for each $j \in S_i'$. Moreover, as the element $j \in S_i \setminus S_i'$ is such that $C_{ij} \neq 0$, we must also have $u_j = a_j$ for each $j \in S_i$ and the copy of H associated to this u contains the edge e. Thus, for each edge colored i and labeled x_i there is a copy of H associated to x in K which contains this edge.

Since there are q^k such edges and there is the same number of copies of H associated to the solution x, no two copies can share the same edge colored i and labeled x_i. By applying the same argument to each of the colors $1, \ldots, m$, we conclude that the q^k copies of H associated to the solution x are edge–disjoint. □

We now proceed with the proof of Theorem 1.

Proof of Theorem 1. Let $\mathcal{H}$ be the family of $(k+1)$–uniform edge colored hypergraphs with m vertices and m edges. Note that $\mathcal{H}$ has a finite number of members. Set $\epsilon' = \epsilon/m$ and, for each $H \in \mathcal{H}$ let δ_H be the quantity obtained from Theorem 4 applied to H. Choose δ to be the smallest such δ_H.

Assume that the matrix A and the vector b have the form described in Lemma 5, and that the number of solutions of the system $Ax = b$ is at most δq^{m-k}. Let H and K be the hypergraphs constructed in this section. By Claims 1 and 2, K contains

at most $\delta q^m \leq \delta_H q^m$ copies of H. By the Removal Lemma for colored hypergraphs (Theorem 4), there is a set E' of edges of K, $|E'| \leq \varepsilon' q^{k+1}$ such that, by deleting the edges in E' from K, the resulting hypergraph is H-free.

The sets X_i' are constructed as follows: if E' contains at least q^k/m edges colored with i and labelled with x_i, remove x_i from X_i. In this way, the total number of elements removed from all the sets X_i together is at most $m \cdot |E'|/q^k \leq \varepsilon q$. Hence, $|X_i \setminus X_i'| \leq \varepsilon q$ as desired. Assume that there is still a solution $x = (x_1, x_2, \ldots, x_m)$ with $x_i \in X_i'$. Consider the q^k edge–disjoint copies of H in K corresponding to x. Since each of these q^k copies contains at least one edge from the set E' and the copies are edge–disjoint, E' contains at least q^k/m edges with the same color i and the same label x_i for some i. However, such x_i should have been removed from X_i. □

5. Proof of Lemma 6

In this section, we prove Lemma 6 by explicitly constructing a matrix C with the required properties.

We first define a family of auxiliary subsets $T_1, \ldots, T_m$. For each i let T_i be the maximum k–subset of $[i-m+1, i]$ in the lexicographic order such that the set of columns $\{A^j,\ j \in T_i\}$ (indices taken modulo m) has rank k.

Lemma 7. *With indices taken modulo m, the following conditions hold:*

(i) *For each $i \in [1, m]$ we have $i \notin T_{i-1}$.*
(ii) *For each $i \in [2, m]$ we have $i \notin T_{i-2}$.*
(iii) *For each i the set T_i is obtained by adding i to T_{i-1} and deleting some element in T_{i-1}.*

Proof. Note that the set of columns $\{A^j,\ j \in [1, m] \setminus \{i\}\}$ span the column space of A. This is clearly so for $k+1 \leq i \leq m$ since $A^1, \ldots, A^k$ is the canonical base. On the other hand, for $1 \leq i \leq k$, it follows from Lemma 5(v) as every row of B has (at least two) nonzero entries. The maximality of T_{i-1} implies (i).

Similarly, it follows from Lemma 5(iv) applied to rows $i-1$ and i with $2 \leq i \leq k$ that the set of columns $\{A^j,\ j \in [1, m] \setminus \{i-1, i\}\}$ also span the column space of A. The same conclusion follows from Lemma 5(v) when $i = k+1$, and it is obvious when $k+2 \leq i \leq m$ since the first k columns of A form the identity matrix. This proves (ii).

By Lemma 5(vi) no column of A is the zero vector, so that $i \in T_i$ for each i. It follows from (i) and the maximality of T_i that the symmetric difference $T_i \Delta T_{i-1}$ has cardinality two. □

We now define the function $g : [1, m] \to [1, m]$ as $g(i) = T_{i-1} \setminus T_i$ (indices taken modulo m). It follows from Lemma 7(iii) that the function g is well defined. Moreover the following holds:

Lemma 8. *We have:*

(i) *The function g is bijective.*
(ii) *There is an ordering of the columns of B such that g is increasing in $[k+1, m]$.*

Proof. If $g(r) = g(s) = i$ for some distinct r and s then i has been deleted twice in the circular process described in Lemma 7(iii) but inserted only once, a contradiction. This proves (i).

We have $T_k = [1, k]$ for every ordering of the columns $A^{k+1}, \ldots, A^m$. For each $i = k+1, \ldots, m]$ we may choose A^i to be a column for which the first nonzero coefficient when expressed as a linear combination of the columns in the base corresponding to T_{i-1} occurs more to the left. This choice minimizes the value of $g(i)$ and makes the function g increasing in $[k+1, m]$. □

We will assume that the last $m-k$ columns of A are ordered in such a way that g is increasing in $[k+1, m]$, a choice which is possible by Lemma 8(ii).

We can now define the matrix C. The j-th column of C has its support in $T_{j-1} \cup \{j\}$. For $i \in T_{j-1}$, the entry C_{ij} is the coefficient of A^i in the expression of A^j in the base $\{A^i,\ i \in T_{j-1}\}$:

$$A^j = \sum_{i \in T_{j-1}} C_{ij} A^i,$$

and $C_{jj} = -1$ (recall that, by Lemma 7(i), we have $j \notin T_{j-1}$.)

Clearly, each column of C belongs to the space of solutions of the system $Ax = 0$, so that Lemma 6 (1) holds.

Since all the elements of T_i, $i \in [k, m-1]$, are in $[1, i]$, the submatrix of C formed by the last $m-k$ columns and the last $m-k$ rows is an upper triangular matrix with nonzero entries on the diagonal which implies that the rank of C is $m-k$. This proves Lemma 6 (2)

By the definition of C the support of column C^j is included in T_j. For $j = k$ we have $T_k = [1, k]$. Since g is increasing in $[k+1, m]$ and, by Lemma 7(iii), each T_j is obtained from T_{j-1} by adding j and deleting $g(j)$, the support of C^j is included in $[g(j), j]$ if $j \in [k+1, m]$. For $j \in [1, k]$, Lemma 7(iii) and the maximality of the T_i's imply that the support of C^j is included in $[1, j] \cup [g(j), m]$.

Let $R \subseteq [1, m] \times [1, m]$ be the area defined by the T_i's, i.e, $(i, j) \in R$ if and only if either $j \in [1, k]$ and $i \in [1, j] \cup [g(j), m]$ or $j \in [k+1, m]$ and $i \in [g(j), j]$ (see Figure 5 for a typical portrait of R.)

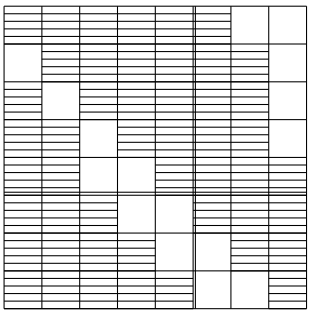

FIGURE 1. An example of the area R in matrix C which corresponds to the permutation $g(1,2,3,4,5,6,7,8) = (3,4,6,7,8,1,2,5)$.

We define the family $\{S_1, \ldots, S_m\}$ of $(k+1)$-subsets of $[1, m]$: S_i is the set of indices j such that $C_{i,j} \in R$. In other words, the sets S_i are obtained by reading off the area R by rows:

$$S_i = \begin{cases} g^{-1}([1, i]) \cup [i, k], & i \in [1, k] \\ g^{-1}(T_i) \cup \{i\}, & i \in [k+1, m]. \end{cases}$$

By the definition of g, the support of the row C_i is contained in S_i for every $i \in [1,m]$ and none of the rows is zero (the entry in the main diagonal is -1).

Let us show that $|S_i| = k+1$.

It follows from the definition of g that $g(i) \notin T_i$. Since g is a bijection, S_i has indeed cardinality $k+1$ for $i \in [k+1,m]$. On the other hand, we can not have $1 \leq g(j) \leq i \leq k$ for $j \in [i,k]$ since this would imply $T_k \neq [1,k]$, a contradiction. Thus $g^{-1}([1,i])$ and $[i,k]$ are disjoint and S_i has also cardinality $k+1$ for $i \in [1,k]$.

Let us now show that the sets S_i are pairwise distinct.

Recall that the region R contains in a column $j \in [1,k]$ the rows $[1,j] \cup [g(j),m]$. It follows from Lemma 7(ii) that $j \notin T_{j-2}$ for $j = 2,...,k+1$, which implies $g(j-1) > j$. Hence S_j does not contain $j-1$ but it does contain j. On the other hand, the column $j \in [k+1,m]$ contains in the region R the rows $[g(j),j]$, so again S_j contains j but does not contain $j-1$.

Let $j < j'$. If $j' \leq k$ then $\{j'-1, j'\} \subseteq [j,k] \subseteq S_j$, which implies $S_j \neq S_{j'}$. If $j' > k$ then, either $j' \notin S_j$ or, as g is increasing in $[k+1,m]$, $\{j'-1, j'\} \subseteq S_j$, which again implies $S_j \neq S_{j'}$.

In order to prove the last part of Lemma 6, we show that the columns $\{C^j,\ j \notin S_i\}$ form a set of $m-k-1$ linearly independent vectors. Together with Lemma 6 (2) and (3), this fact implies Lemma 6 (4) and completes the proof of the Lemma.

Let $C' = \{C^j :\ j \notin S_i\}$ be the submatrix of C formed by the columns with indices not in S_i. We divide this matrix into four parts: the upper left $UL = \{C_{rs} :\ r < i,\ s \in [1,i] \setminus S_i\}$ formed by the first $i-1$ rows of C and the columns with index at most i, the upper right $UR = \{C_{rs} :\ r < i,\ s \in [i+1,m] \setminus S_i\}$ formed by the same rows and the remaining columns, the lower right $LR = \{C_{rs} :\ r \geq i,\ s \in [1,i] \setminus S_i\}$ formed by the last $m-i+1$ rows and the columns with index at most i and the lower left $LR = \{C_{rs} :\ r \geq i,\ s \in [i+1,m] \setminus S_i\}$ with the remaining entries.

By our construction of the matrix C, UR is an all-zero matrix, while, as discussed in the proof of Lemma 6 (2), the columns C^j with $j \in [i+1,m] \setminus S_i$ are linearly independent because the columns C^j, $j \in [k+1,m]$, are linearly independent. On the other hand, again by the construction of C, UL is an upper triangular matrix (maybe with the steps higher than one). It follows that the columns of C' are linearly independent. This completes the proof of Lemma 6.

Acknowledgments

We would like to thank Vojtěch Rödl, Mathias Schacht and Balázs Szegedy for helpful discussions and comments. We also want to thank an anonymous referee for her useful comments which helped us to significantly improve the presentation of the paper.

References

[1] T. Austin and T. Tao, On the testability and repair of hereditary hypergraph properties, arxiv0801.2179v1.

[2] P. Candela, On systems of linear equations and uniform hypergrpahs, manuscript, 2008.

[3] P. Erdos, P. Frankl, and V. Rdl. The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent. Graphs Combin. **2** (1986), no. 2, 113–121.

[4] P. Frankl, V. Rödl. Extremal problems on set systems. Random Structures Algorithms 20 (2002), no. 2, 131–164.

[5] W. T. Gowers. Hypergraph regularity and the multidimensional Szemerédi theorem. Ann. of Math. (2) 166 (2007), no. 3, 897–946.

[6] B. Green. A Szemerédi-type regularity lemma in abelian groups, with applications. Geometric and Functional Analysis 15(2) (2005), 340–376.
[7] D. Král', O. Serra, L. Vena. A combinatorial proof of the Removal Lemma for groups. J. Combin. Theory Ser. A 116 (2009), no. 4, 971–978.
[8] D. Král', O. Serra, L. Vena. A removal lemma for linear systems over finite fields. Proc. VI Jornadas Matemàtica Discreta y Algorítmica, Ediciones y Publicaciones de la UdL, 2008, 417–424.
[9] J. Komlós, M. Simonovits. Szemerédi's regularity lemma and its applications in graph theory. Combinatorics, Paul Erdős is eighty, Vol.2 (Keszthely, 1993), 295-352, Bolyai Soc. Math. Stud., 2, János bolyai Math Soc., Budapest, 1996.
[10] J. Komlós, A. Shokoufandeh, M. Simonovits, E. Szemerédi. The regularity lemma and its applications in graph theory, Theoretical aspects of computer science (Tehran, 2000), 84–112, Lecture Notes in Comput. Sci., **2292**, Springer, Berlin, (2002).
[11] B. Nagle, V. Rödl, M. Schacht. The counting lemma for regular k-uniform hypergraphs. Random Structures Algorithms 28 (2006), no. 2, 113–179.
[12] V. Rödl, J. Skokan. Applications of the Regularity Lemma for Uniform Hypergraphs. Random Structures Algorithms 28 (2006), no. 2, 180–194.
[13] I.Z. Ruzsa, E. Szemerédi. Triple systems with no six points carrying three triangles. Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, pp. 939–945, Colloq. Math. Soc. János Bolyai, 18, North-Holland, Amsterdam-New York, 1978.
[14] A. Shapira. A proof of Green's conjecture regarding the removal properties of sets of linear equations. Submitted, available as arXiv:0807.4901v2 [math.CO].
[15] A. Shapira. Green's conjecture and testing linear-invariant properties Proceedings of the 41st annual ACM symposium on Theory of computing (2009) 159–166.
[16] E. Szemerédi. On sets of integers containing no k elements in arithmetic progression Acta. Arith. **27** (1975), 299–345.
[17] B. Szegedy. The Symmetry Preserving Removal Lemma. manuscript, preprint available as arXiv:0809.2626.
[18] T. Tao. A variant of the hypergraph removal lemma. J. Combin. Theory Ser. A, **113** (2006), 1257–1280.
[19] P. Varnavides. On certain sets of positive density, J. London Math. Soc., **34** (1959), 358–360.

Institute for Theoretical Computer Science (ITI), Faculty of Mathematics and Physics, Charles University, Malostranské náměstí 25, 118 00 Prague, Czech Republic.
E-mail address: kral@kam.mff.cuni.cz

Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
E-mail address: oserra@ma4.upc.edu

Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya
E-mail address: lvena@ma4.upc.edu