On the Removal Lemma for linear systems over Abelian groups

Daniel Král'* Oriol Serra† Lluís Vena‡

Abstract

In this paper we present an extension of the removal lemma to integer linear systems over abelian groups. We prove that, if the k–determinantal of an integer $(k\times m)$ matrix A is coprime with the order n of a group G and the number of solutions of the system $Ax=b$ with $x_1 \in X_1, \ldots, x_m \in X_m$ is $o(n^{m-k})$, then we can eliminate $o(n)$ elements in each set to remove all these solutions.

1 Introduction

In 2005 Green [6] introduced the so-called Removal Lemma for Groups. It roughly says that if a linear equation with integer coefficients

$$a_1x_1 + a_2x_2 + \cdots + a_mx_m = 0$$

has not many solutions with variables taking values from given subsets $X_1, \ldots, X_m$ of a finite Abelian group G, then one can delete all these solu-

*Department of Applied Mathematics and Institute for Theoretical Computer Science (ITI), Faculty of Mathematics and Physics, Charles University. E-mail: kral@kam.mff.cuni.cz. Institute for Theoretical Computer Science (ITI) is supported as project 1M0545 by Czech Ministry of Education.

†Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya. E-mail: oserra@ma4.upc.edu. Supported by the Catalan Research Council under project 2008SGR0258 and the Spanish Research Council under project MTM2008-06620-C03-01.

‡Department of Mathematics, University of Toronto, Canada. Supported by a University of Toronto Graduate Fellowship.

tions by removing a small quantity of elements in each subset. This result mimics the Removal Lemma for Triangles (see [11]) in graphs, where it takes the name from.

The Removal Lemma for Groups has been extended to one equation with elements in non-necessarily Abelian groups (see [8]) and, by confirming a conjecture of Green [6], to linear systems over Finite Fields independently by Shapira [12] and the authors [9].

Shapira [12] asked for an extension of the result to Abelian groups. This work attempts to answer this question.

Recall that the k-th determinantal $d_k(A)$ of an integer matrix A is the greatest common divisor of all the $k \times k$ submatrices of A. Our main result is the following:

Theorem 1. *Let A be an integer $(k \times m)$ matrix, $m \geq k$. For every real positive number $\epsilon > 0$ there exists a $\delta(\epsilon, A) > 0$ such that the following holds.*

For every Abelian group G of order n coprime with $d_k(A)$, for every family of subsets $X_1, \ldots, X_m$ of G and for every vector $b \in G^k$, if the linear system $Ax = b$ has at most δn^{m-k} solutions with $x_1 \in X_1, \ldots, x_m \in X_m$ then there are sets $X_1' \subset X_1, \ldots, X_m' \subset X_m$ with $|X_i'| \leq \epsilon n$, for all i, such that there is no solution of the system with $x_1 \in X_1 \setminus X_1', \ldots, x_m \in X_m \setminus X_m'$.

In the little 'o' notation, Theorem 1 states that, if an integer linear system over an Abelian group of order n (with the condition that the determinantal of the matrix is coprime with the order of the group), has $o(n^{m-k})$ solutions, then we can destroy all the solutions by removing $o(n)$ elements in each set.

Let us remark that the condition over the determinantal $d_k(A)$ in the statement of Theorem 1 indicates that the system is, in a sense, well defined. It is analogous to the condition in the version of Theorem 1 for linear systems over finite fields that the matrix A has full rank.

A general framework for the study of this type of results is discussed by Szegedy [13]. The author proves a Symmetry Removal Lemma and applies it to give a diagonal version of the Szemerédi Theorem on arithmetic progressions in Abelian groups. Our work follows the direction of our original argument for the nonabelian case presented in [8], and it provides a general answer for linear systems $Ax = b$, which includes the case of arithmetic progressions [13, Theorem 3].

The proof of Theorem 1 uses the Removal Lemma for colored hypergraphs. The extension of the Removal Lemma to hypergraphs has been obtained by several authors, see Austin and Tao [1], Elek and Szegedy [3], Gowers [5], Ishigami [7] or Nagle, Rödl and Schacht [10].

An r-colored k-uniform hypergraph is a pair (V, E) formed by a set V of vertices and a subset $E \subset \binom{V}{k}$ of edges which are k–subsets of vertices, and a map $c : E \to [1, r]$ which assigns 'colors' to the edges. Given two colored k–uniform hypergraphs H and K, we say that K contains a copy of H if there is an injective homomorphism $f : H \mapsto K$, a map from the set of vertices of H to the set of vertices of K whose natural extension to edges preserves edges and colors. We also say that K contains two disjoint copies of H if there are two injective homomorphisms $f, f' : H \mapsto K$ such that $f(E(H)) \cap f'(E(H)) = \emptyset$. The hypergraph K is H–free if it contains no copy of H. We shall use the following version of the hypergraph Removal Lemma, which follows, for instance, from [1, Theorem 2.1].

Theorem 2. *For every positive integers $m \geq k \geq 2$ and every $\epsilon > 0$ there is a $\delta > 0$ depending on m, k and ϵ such that the following holds.*

Let H and K be colored k-uniform hypergraphs with $m = |V(H)|$ and $M = |V(K)|$ vertices respectively. 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 such that the hypergraph K' with edge set $E(K) \setminus E'$ is H–free.

2 Circular Unimodular Matrices

In this section we will prove Theorem 1 in the particular case of homogeneous linear systems with what we call standard circular unimodular matrices, which enjoy some useful particular properties. We will show in Section 3 how the statement extends to the general case.

Throughout the paper A_i denotes the i–th row of a matrix A and A^j its j–th column. Recall that a square integer matrix is unimodular if it has determinant ± 1.

We say that a $(k \times m)$ integer matrix is standard circular unimodular if the following properties hold:

(U1) $A = (I_k|B)$, where I_k denotes the identity matrix of order k.

(U2) For each $j = 1, \ldots, m$, the determinant formed by k consecutive columns in the circular order, $\{A^{j+1}, A^{j+2}, \ldots, A^{j+k}\}$ is ± 1, where the superscripts are taken modulo m.

We simply call matrices satisfying property U2 *circular unimodular*. Note that property U1 can always be imposed to a circular unimodular matrix by using elementary matrix transformations. The next key Lemma proves Theorem 1 for circular unimodular matrices by constructing an hypergraph associated to a given linear system. The approach is similar to the one by Candela [2] and by the authors [8].

Lemma 3. *Let A be a $(k \times m)$ circular unimodular matrix with $m \geq k+2$. For each $\epsilon > 0$ there is a $\delta(\epsilon, A) > 0$ such that the following holds.*

For every Abelian group G of order n and every collection of subsets $X_1, \ldots, X_m \subset G$, if the number of solutions of the system $Ax = 0$ with $x \in \prod_{i=1}^m X_i$ is at most δn^{m-k}, then there are subsets $X_i' \subset X_i$ with $|X_i'| < \epsilon n$ for all i such that there is no solution of the system $Ax = 0$ with $x \in \prod_{i=1}^m (X_i \setminus X_i')$.

Moreover, if we have $X_j = G$, for $j \in I$, where $I \subset \{1, \ldots, m\}$ has cardinality $|I| \leq k$, then we can choose the sets X_i' in such a way that $X_j' = \emptyset$ for each $j \in I$.

Proof. We start by defining an integer $(m \times m)$ matrix C from which we will construct a pair of colored hypergraphs H and K. The purpose of this construction is to establish a correspondence between solutions of the system $Ax = 0$ with copies of H in K.

By property U2, the j–th column of A can be written, for every j, as an integer linear combination of the preceding k columns in the circular ordering:

$$A^j = \sum_{i=j-k}^{j-1} C_{i,j} A^i,$$

where the superscript i is taken modulo m.

For $j = 1, 2, \ldots, m$ we let $C_{j,j} = -1$ and, if i does not belong to the circular interval $[j-k, j]$, then we set $C_{i,j} = 0$. Thus,

$$\sum_i C_{i,j} A^i = 0,\ j = 1, 2, \ldots, m. \tag{1}$$

Notice that, since all the determinants of k consecutive columns of A in the circular ordering are ± 1, the coefficients of C are integers (apply the Cramer's rule to solve the corresponding linear systems). By the same reason, we have

$$C_{j-k,j} = \pm 1,$$

since the determinants of the matrices formed by the columns $A^{j-k+1}, \ldots, A^j$ and by the columns $A^{j-k}, \ldots, A^{j-1}$ are both ± 1.

The integer $(m \times m)$ matrix $C = (C_{i,j})$ will be used to define our hypergraph model for the given linear system.

Let H be a $(k+1)$-uniform colored hypergraph with m vertices labelled $\{1, 2, \ldots, m\}$. The edges of H are the m "cyclic" $(k+1)$–subsets

$$\{1, \ldots, k+1\}, \{2, \ldots, k+2\}, \ldots, \{m, 1, \ldots, k\},$$

(entries taken modulo m). The i-th edge $\{i, i+1, \ldots, i+k\}$ is colored with color i. Since $m \geq k+2$, H contains m different edges of mutually different colors.

Let K be a $(k+1)$-uniform colored hypergraph with vertex set $G \times [1, m]$. For each element $a_i \in X_i$, the $(k+1)$–subset $\{(g_i, i), \ldots, (g_{i+k}, i+k)\}$ form an edge labelled a_i and colored with color i if

$$a_i = \sum_{j=i}^{i+k} C_{i,j} g_j. \tag{2}$$

Thus the edges of K bear both, a color and a label. Note that, for each fixed $a_i \in X_i$, the system (2) has n^k solutions. Indeed, since $C_{i,i} = \pm 1$, we can fix arbitrary values $g_{i+1}, \ldots, g_{i+k}$ and get a value for g_i satisfying the equation. Therefore each element $a_i \in X_i$ gives rise to n^k edges colored i and labeled a_i.

We next show that each solution to $Ax = 0$ creates n^k edge-disjoint copies of the hypergraph H inside K and, also, that each copy of H inside K comes from a solution of the system $Ax = 0$.

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

Proof. The copy H' has an edge of each color and is supported over m vertices. Since the edge colored i contains a vertex in $G \times \{i\}$, then the copy H' has one vertex on each $G \times \{i\}$, $1 \le i \le m$. Hence the vertex set of H' is of the form $\{(g_1, 1), (g_2, 2), \dots, (g_m, m)\}$ for some $g_1, \dots, g_m \in G$. If the edge $((g_i, i), \dots, (g_{i+k}, i + k))$ colored i in H' has label x_i then, by the construction of K, we have $x_i = \sum_s C_{i,s} g_s$. Therefore, it holds that $Cg = x$ where $g = (g_1, g_2, \dots, g_m)$. Hence, as all the columns in C are in the kernel of A, we have $0 = ACg = Ax$ and x is a solution of the system. □

Claim 2. *For any solution $\alpha = (\alpha_1, \dots, \alpha_m)$ of the system $Ax = 0$ with $\alpha_i \in X_i$, there are precisely n^k edge–disjoint copies of the edge–colored hypergraph H in the hypergraph K with edges labelled with $\alpha_1, \dots, \alpha_m$.*

Proof. Fix a solution $\alpha = (\alpha_1, \dots, \alpha_m)$ of $Ax = 0$ with $\alpha_i \in X_i$, $1 \le i \le m$.

Observe that, by property U2, α is uniquely determined by any of its subsequences $(\alpha_i, \alpha_{i+1}, \dots, \alpha_{i+m-k-1})$ of $m - k$ consecutive coordinates in the circular ordering.

By the construction of the matrix C, its i-th row C_i has an entry ± 1 in the i–th column and has its support contained in columns $C^i, C^{i+1}, \dots, C^{i+k}$ (where the superscripts are taken modulo m.) Therefore, the $m-k$ columns of C with indices in $[1, m] \setminus [i + 1, \dots, i + k]$ have a unique nonzero entry in the main diagonal, which is ± 1.

With the previous remark in mind, we observe that, for every choice of a vector $(g_{i+1}, \dots, g_{i+k}) \in G^k$ (subscripts modulo m), there is a unique vector $(g_{i+k+1}, \dots, g_{i-1}, g_i) \in G^{m-k}$ which satisfies the system $Cg = \alpha$, where $\alpha = (\alpha_1, \dots, \alpha_m)$ is the solution of the system $Ax = 0$ with $\alpha_i \in X_i$ we have fixed from the beginning and $g = (g_1, g_2, \dots, g_m)$. Indeed, for each t, once the values $(g_{i+1-t}, g_{i+2-t}, \dots, g_{i+k-t})$ have been found, we can determine g_{i-t} from the equation

$$\alpha_{i-t} = \sum_{s=i-t}^{i+k-t} C_{i-t,s} g_s, \tag{3}$$

since $C_{i-t,i-t} = \pm 1$. In this way, starting with the vector $(g_{i+1}, \ldots, g_{i+k-1}, g_{i+k}) \in G^k$ and $m-k$ consecutive elements of α, $\{\alpha_{i+k+1}, \ldots, \alpha_{i-1}, \alpha_i\}$, we find a unique m-dimensional vector $g = (g_1, \ldots, g_m)$. Observe that $\beta = Cg \in G^m$ satisfies $A\beta = A(Cg) = (AC)g = 0g = 0$. Therefore β is a solution of the system $Ax = 0$ which shares $m-k$ consecutive values with the given solution α, hence $\beta = \alpha$. It follows that the equations (3) hold for all t. Since these are the defining equations (2) for the k–tuple $(g_i, i), \ldots, (g_{i+k}, i+k)$ to be an edge of K colored i and labeled x_i, we conclude that each vector $(g_{i+1}, \ldots, g_{i+k}) \in G^k$ defines uniquely a copy of H in K. Hence the solution α induces n^k copies of H in K.

Recall that each entry $\alpha_i \in X_i$ of α gives rise to n^k edges labeled α_i in the hypergraph K. On the other hand each of these edges belong to a unique copy of H inside K related to the solution α. Since this holds for each of the edges and for each α_i, $1 \leq i \leq m$, we conclude that the n^k copies of H with edges labelled with $\alpha_1, \ldots, \alpha_m$ are edge-disjoint. □

Claims 1 and 2 show that there is a bijection between the solutions of the system $Ax = 0$ and the copies of H inside K.

We now proceed with the proof of Lemma 3. Given $\epsilon > 0$ let $\delta > 0$ be the value given by the Removal Lemma of colored hypergraphs (Theorem 2) for the positive integers $m, k+1$ and $\epsilon' = \epsilon/m > 0$. If the number of solutions of the system $Ax = 0$ is at most δn^{m-k}, it follows from Claims 1 and 2, that K contains δn^m copies of H. By Theorem 2, there is a set E' of edges of K with size $\epsilon' n^{k+1}$ such that, by deleting the edges in E' from K, the resulting hypergraph is H-free.

The subsets $X_i' \subset X_i$ of removed elements are constructed as follows: if E' contains at least n^k/m edges colored with i and labeled with x_i, we remove x_i from X_i (that is, $x_i \in X_i'$.) In this way, the total number of elements removed from all the sets X_i together is at most $m\epsilon' n = \epsilon n$. Hence, $|X_i'| \leq \epsilon n$ as desired. Suppose that there is still a solution $x = (x_1, x_2, \ldots, x_m)$ with

$x_i \in X_i \setminus X_i'$. Consider the n^k edge–disjoint copies of H in K corresponding to x. Since each of these n^k copies contains at least one edge from the set E' and the copies are edge–disjoint, E' contains at least n^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, a contradiction.

It remains to show the last part of Lemma 3. Let I be a subset of $[1, m]$ with $|I| \leq k$, and suppose that $X_j = G$ for each $j \in I$. Let L be the subgraph of H formed by all the edges in H except the ones colored with $i \in I$. Note that H contains a single copy of L. Since every vertex of H belongs to $(k+1)$ edges, the subgraph L has no isolated vertices. It follows that a copy L' of L in K has precisely one vertex in $G \times \{i\}$ for each $i = 1, 2, \ldots, m$. By the construction of K, there is at most one copy H' of H in K containing L', namely the one whose labels are given by equation (2) given the g_i's. Since $X_j = G$ for each $j \in I$, then the label of each missing edge in L', given by this equation, belongs to the corresponding set X_j, thus such an edge is indeed present in K. Hence, every copy of L in K can be uniquely extended to a copy of H. Thus, K contains as many copies of H as of L. We can apply Theorem 2 to L in the above argument to remove all copies of L by removing only elements from sets X_i with $i \in \{1, \ldots, m\} \setminus I$. This completes the proof. □

The condition $m \geq k + 2$ in the hypothesis of Lemma 3 has been used in the proof for the construction of the hypergraphs associated to the linear system. However, this condition is not restrictive for the proof of Theorem 1; in the remaining cases (when m is k or $k+1$), we apply the following lemma:

Lemma 4. *Let $A = (I_k|B)$ be a $(k \times m)$ integer matrix. If $m = \{k, k+1\}$ then the statement of Theorem 1 holds for A.*

Proof. For $m = k$ the system has a unique solution and there is nothing to prove. Suppose that $m = k + 1$. Then, for each element $\alpha \in X_{k+1}$ there is at most one solution to the system $Ax = b$ with last coordinate $x_{k+1} = \alpha$. Let X_{k+1}' be the set of elements $\alpha \in X_{k+1}$ such that $x_{k+1} = \alpha$ is the last coordinate of some solution x. Since there are at most δn solutions we have $|X_{k+1}'| \leq \delta n$ and we are done by removing the set X_{k+1}'. Thus the statement of Theorem 1 holds with $\delta = \epsilon$. □

3 A reduction Lemma

In this section we prove some technical lemmas that will allow us to derive Theorem 1 from Lemma 3 via a series of transformations to the given linear system.

Recall that the adjugate matrix of L, denoted by $\mathrm{adj}(L)$, is the matrix C with $C_{i,j} = (-1)^{i+j} M_{j,i}(L)$, where $M_{j,i}(L)$ is the determinant of the matrix L with the row j and the column i deleted.

Throughout the section G denotes an Abelian finite group of order n. For an integer a coprime with the order n of G the map $g \mapsto ag$ is an automorphism of the group. We will also denote by a this automorphism and by a^{-1} its inverse. Observe that if an $(r \times r)$ integer matrix L has determinant $a = \det L$ coprime with n then the action $x \mapsto Lx$ of L on G^r is invertible with $L^{-1}x = a^{-1}(\mathrm{adj}(L)x)$. Thus the linear system $Lx = b$ has the unique solution $x = L^{-1}b$. By abuse of notation, in what follows we write $L^{-1}b$ and, for a matrix M with appropiate dimensions, $L^{-1}M$, in the sense that division by a means the action of the automorphism a^{-1}.

We let A denote a $(k \times m)$ integer matrix such that its k-th determinantal $d_k(A)$ satisfies $\gcd(d_k(A), n) = 1$. Let $b \in G^k$ and let $\mathcal{X} = X_1 \times X_2 \times \cdots \times X_m$ be an m–tuple of subsets of G. We say that the triple $\{A, b, \mathcal{X}\}$ is a *restricted system*. A solution of the restricted system $\{A, b, \mathcal{X}\}$ is a vector $x = (x_1, \ldots, x_m) \in G^m$ such that $Ax = b$ and $x_i \in X_i$, $i = 1, 2, \ldots, m$.

A restricted system $\{A', b', \mathcal{Y}\}$, where A' is a $(k' \times m')$ integer matrix and $\mathcal{Y} = Y_1 \times Y_2 \times \cdots \times Y_{m'}$, is an *extension* of $\{A, b, \mathcal{X}\}$ if the following two conditions hold:

- E1: $k' \geq k$, $m' \geq m$, $m' - k' = m - k$, and
- E2: There is a subset $I_0 \subset [1, m']$ with cardinality $|I_0| = m$ a bijection $\sigma : I_0 \to [1, m]$ and maps $\phi_i : Y_i \to X_{\sigma(i)}$ such that the map $\phi : \mathcal{Y} \to \mathcal{X}$ with $(\phi(y))_i = \phi_{\sigma^{-1}(i)}(y_{\sigma^{-1}(i)})$ induces a bijection between the set of solutions of $\{A', b', \mathcal{Y}\}$ and the set of solutions of $\{A, b, \mathcal{X}\}$. Moreover, for each $i \in [1, m'] \setminus I_0$, we have $Y_i = G$.

Thus, an extension $\{A', b', \mathcal{Y}\}$ of $\{A, b, \mathcal{X}\}$ has the same number of solutions and one can define a map ϕ such that, if $\{A', b', \mathcal{Y}\setminus\mathcal{Y}'\}$ has no solutions, then $\{A, b, \mathcal{X}\setminus\phi(\mathcal{Y}')\}$ has no solutions either (here $\mathcal{Y}\setminus\mathcal{Y}'$ stands for $\prod_{i=1}^{m'} Y_i \setminus Y_i'$ and $\mathcal{X}\setminus\phi(\mathcal{Y}')$ refers to $\prod_{i=1}^{m} X_i \setminus \phi_{\sigma^{-1}(i)}(Y'_{\sigma^{-1}(i)}.)$

When $\{A', b', \mathcal{Y}\}$ is an extension of $\{A, b, \mathcal{X}\}$ with $k = k'$, any bijection for σ, and the ϕ_i's are bijective for each i, we say that the two systems are equivalent.

The purpose of this section is to show that any restricted system which fulfills the hypothesis of Theorem 1 can be extended to an homogeneous one with a circular unimodular matrix. This will lead to a proof of Theorem 1 from Lemma 3.

We first show that the matrix A can be enlarged to an integer square matrix M of order m such that $\det(M) = d_k(A)$. The following Lemma uses the ideas of Zhan [14] and Fang [4] to extend partial integral matrices to unimodular ones. We include the proof of the simpler version we need for our purposes.

Lemma 5 (Matrix extension)**.** *Let M be an $r \times s$ integer matrix, $s \geq r$. Let d_M denote the greatest common divisor of the determinants of the $\binom{s}{r}$ square $(r \times r)$ submatrices of M.*

There is an $s \times s$ integer matrix $\overline{M}$ such that

(i) *$\overline{M}$ contains M in its r first rows, and*

(ii) $\det(\overline{M}) = d_M$.

Proof. Let $S = U^{-1}MV^{-1}$ be the Smith normal form of M, where U and V are unimodular matrices. We have $S = (D|0)$, where D is an $(r \times r)$ diagonal integer matrix with $|\det(D)| = |d_M|$ and 0 is an all–zero $(r \times (s-r))$ matrix.

Recall that U and V are the row and column operations respectively which transform M into S. Observe that the row operations do not modify the value of the determinant of any $(r \times r)$ square submatrix of M. The column operations may modify individual determinants but do not change the value of d_M.

Let $\overline{S}$ be the matrix:

$$\overline{S} = \begin{pmatrix} D & 0 \\ 0 & I_{s-r} \end{pmatrix},$$

where I_k denotes the identity matrix of order k. We have $\det(\overline{S}) = \det(D) = d_M$.

Then, if we let $\overline{V} = V$ and

$$\overline{U} = \begin{pmatrix} U & 0 \\ 0 & I_{s-r} \end{pmatrix},$$

we obtain the matrix

$$\overline{M} = \overline{U}\,\overline{S}\,\overline{V}$$

which clearly (i) contains M as a submatrix in its first r rows, and (ii) $\det(\overline{M}) = \det(\overline{S}) = d_M$, since $\overline{U}$ and $\overline{V}$ are still unimodular. □

We say that the restricted system $\{A, b, \mathcal{X}\}$ is *thin* if the set of solutions is a subset of $X_1 \times \cdots \times X_{i-1} \times \{\gamma_j\} \times X_{i+1} \times \cdots \times X_m$, for some j and $\gamma_j \in X_j$. Note that the statement of Theorem 1 is obvious if the system is thin since it suffices to delete the element γ_j to remove all solutions. Thus there is no loss of generality in assuming that our restricted system is not thin.

Lemma 6. *The restricted system $\{A, b, \mathcal{X}\}$ is either thin or it has an extension $\{A', b', \mathcal{Y}\}$ such that*

(i) $k' = m$ *and* $m' = 2m - k$*;*

(ii) *the matrix A' has the form $A' = (I_{k'}|B)$;*

(iii) $b' = 0$*;*

(iv) $\gcd(B_i) = 1$*, where B_i denotes the i–row of the submatrix B and*

(v) $\max_{i,j}\{|A'_{i,j}|\}$ *depends on the entries of A but not on the group G.*

(vi) *the sets restricting variables corresponding to the columns of B in $\mathcal{Y}$ are equal to the whole group G.*

Proof. By using Lemma 5 we extend the matrix A into an $m \times m$ square matrix

$$M = \begin{pmatrix} A \\ E \end{pmatrix}$$

with determinant $\det(M) = d_k(A)$. We complete the square matrix M to the $m \times (2m-k)$ matrix

$$M' = \begin{pmatrix} A & 0 \\ E & I_{m-k} \end{pmatrix} = (M|B').$$

We now consider the restricted system $\{M', b', \mathcal{X}'\}$ where $b' = (b, 0)$ is obtained from b by adding zeros in the last $m-k$ coordinates and

$$X'_i = \begin{cases} X_i, & 1 \le i \le m; \\ G, & m+1 \le i \le 2m-k. \end{cases}$$

By letting $I_0 = [1, m]$ and σ and ϕ_i be the identity maps we see that y is a solution of $\{M', b', \mathcal{X}'\}$ if and only if $x = \phi(y')$ is a solution of $\{A, b, \mathcal{X}\}$, where $y' = (y_i : \ i \in I_0)$. Therefore $\{M', b', \mathcal{X}'\}$ is an extension of the original system.

Let $U = \mathrm{adj}(M)$ denote the adjugate of M. Since $a = d_k(A)$ is relatively prime with n, we get an equivalent restricted system $\{M'', b'', \mathcal{X}'\}$ by setting

$$M'' = (UM|UB') = (a \cdot I_m|UB'),\ b'' = Ub''$$

and, by replacing each X'_i, for $i \in [1, m]$, by $\bar{X}''_i = a^{-1}X'_i$ and $\bar{X}''_i = X'_i$, for $i \in [m+1, 2m-k]$, we get a an equivalent system of the form $\{(I_m|B''), b'', \bar{\mathcal{X}}''\}$ where $B'' = UB'$. The system is equivalent since the matrix U is invertible in G.

At this point we can erase the independent vector b by letting $X''_i = \bar{X_i}'' - b''_i$ for $i = 1, \ldots, m$ and leaving the other sets untouched. The solutions of the homogeneous system $(I_m|B'')x = 0$ with $x_i \in X'''_i$ are in bijective correspondence with the solutions of $M''x = b''$ with $x_i \in X''_i$. So $\{(I_m|B''), 0, \mathcal{X}''\}$ is a system equivalent to $\{(I_m|B''), b'', \bar{\mathcal{X}}''\}$, which fulfills conditions (i)-(iii) of the Lemma.

We observe that, if $B^{''}_j = 0$ for some j, then the j-th equation implies $x_j = 0$. Thus, the solution set of $\{(I_m|B''), b'', \bar{\mathcal{X}}''\}$ is inside $X^{''}_1 \times \cdots \times X^{''}_{j-1} \times \{0\} \times X^{''}_{j+1} \times \cdots \times X^{''}_{m'}$, which implies that the solution set for the original system is inside $X_1 \times \cdots \times X_{j'-1} \times \{\gamma_{j'}\} \times X_{j'+1} \times \cdots \times X_m$, for some $\gamma_{j'} \in X_{j'}$. Thus, if $B^{''}_j = 0$, then the system is thin. Therefore we can assume that all the rows in $B^{''}$ are non–zero.

Suppose that $\gcd(B''_i) = s > 1$, where B''_i denotes the i–th row of B''. Then the i–th coordinate y_i, $i \in [1, m]$, of a solution of $(I_m|B'')y = 0$ belongs to the subgroup $s \cdot G$ of G. Thus we may assume that $X''_i \subset s \cdot G$. Let $Y_i = s^{-1}(X''_i)$, where now s^{-1} denotes the preimage of the canonical projection $s : G \to s \cdot G$ defined by $s(g) = sg$, and divide the entries of the i–row B''_i by s. In this way we obtain an extension of $\{(I_m|B''), 0, \mathcal{X}''\}$ where the map $\phi_i : Y_i \to X_i$, $i \in [1, m]$, is the multiplication by s. By repeating the same procedure with each row of B'' we eventually obtain an extension $\{A', 0, \mathcal{Y}\}$ satisfying the conditions (i)-(iv) of the Lemma. Moreover, since all operations performed on A to obtain A' depend only on the entries of A and not on G, the condition (v) also holds. The condition (vi) is satisfied as we have added the last variables corresponding to the columns in B and they run over the full group G. This completes the proof. □

Our final step is to show that, if the restricted system $\{A, 0, \mathcal{X}\}$, where A satisfies the conclusions of Lemma 6, is non–thin, then it admits an extension with a circular unimodular matrix.

Lemma 7. *Let $\{A, 0, \mathcal{X}\}$ be a non–thin restricted system where $A = (I_k|B)$ and $\gcd(B_i) = 1$ for every row i. There is an extension $\{A', 0, \mathcal{X}'\}$ with $k' = k'(A)$ depending only on the entries of A such that all matrices formed by k' consecutive columns of A' in the circular ordering are unimodular. Moreover, up to a reordering on the indices j, $\mathcal{X}' = \mathcal{X} \times \prod_{j=m+1}^{k'+m-k} G$.*

Proof. The stated extension is based on the following construction. Let M be a unimodular matrix of order $m-k$. By adding to M a row at the bottom of the form $M_1 + \sum_{i=2} \lambda_i M_i$, where $\lambda_i \in \mathbb{Z}$ and M_i denotes the i–th row of M, the last $(m-k)$ rows of the resulting matrix form a unimodular matrix. By choosing appropriate row operations at each step we may transform M into the identity matrix. By putting each such transformation as a new row at the bottom of M we obtain a matrix of the form

$$M' = \begin{pmatrix} M \\ T \\ I_{m-k} \end{pmatrix}$$

such that every $(m-k) \times (m-k)$ submatrix of M' formed by consecutive rows is unimodular. The same procedure can be repeated by adding rows to the top of M to obtain a matrix of the form

$$M'' = \begin{pmatrix} I_{m-k} \\ S \\ M \\ T \\ I_{m-k} \end{pmatrix}$$

and again every $(m-k) \times (m-k)$ submatrix of M'' formed by consecutive rows is unimodular. Note that the dimensions of S and T depend on the number of row operations needed to transform M into the identity matrix. These operations involve performing an Euclidian algorithm on the entries of M and its number can be upper bounded by five times the logarithm of the largest entry in the matrix.

We apply the above procedure to the matrix B in the following manner. As each row B_i of the submatrix B is such that $\gcd(B_i) = 1$, we can apply Lemma 5 to the row B_i, by using $M = B_i$, $r = 1$ with $s = m - k$, and obtain a $(m-k) \times (m-k)$ square matrix $\overline{B_i}$ with determinant ± 1. Thus, by applying the above procedure to each of the resulting matrices $\overline{B_1}, \ldots, \overline{B_k}$ we may construct the following $k' \times (m-k)$ rectangular matrix:

$$B' = \begin{pmatrix} I_{m-k} \\ S_1 \\ \overline{B_1} \\ T_1 \\ I_{m-k} \\ S_2 \\ \overline{B_2} \\ T_2 \\ I_{m-k} \\ \cdots \\ I_{m-k} \\ S_k \\ \overline{B_k} \\ T_k \\ I_{m-k} \end{pmatrix},$$

for some k' depending on B. Let

$$A' = (I_{k'} | B').$$

Observe that every set of k' consecutive columns in the circular order in A' form a unimodular matrix. To check this, let $M(i)$ be the square submatrix formed by k' consecutive columns of A' in the circular order starting with the i–th column.

Since the matrix A' has the form

$$A' = \left(I_{k'} \;\middle|\; \begin{matrix} I_{m-k} \\ X \end{matrix} \right)$$

for some matrix X, then each matrix $M(i)$ for $i = 1, \ldots, m-k$ is a circular permutation of a lower triangular matrix with all ones in the diagonal. Hence $M(i)$ is unimodular for these values of i.

For the remaining values of i, $\det M(i)$ equals, up to a sign, the determinant of a submatrix of B' formed by $m-k$ consecutive rows which, by construction, is unimodular. More precisely, $\det M((m-k)+t)$ equals, up to a sign, the determinant of the matrix formed by the rows $B'_{t+1}, B'_{t+2}, \ldots, B'_{t+(m-k)}$.

In order to complete the proof of the Lemma we must construct the family $\mathcal{X}'$ of $m' = k' + m - k$ sets. Let $I_0^1 \subset [1, m']$ be the set of subscripts for which the i–row of B' corresponds to a row $\sigma(i)$ of the original matrix B and let $I_0^2 = [m' - (m-k) + 1, m']$. Let $I_0 = I_0^1 \cup I_0^2$. By setting $X'_i = X_{\sigma(i)}$ for $i \in I_0^1$, $X'_i = X_{i-m'+m}$ for $i \in I_0^2$, and $X'_i = G$ otherwise, we get an extension $(A', 0, \mathcal{X}')$ of the given restricted system with

$$\phi : \prod_{i=1}^{k} X'_{\sigma^{-1}(i)} \times \prod_{i=k+1}^{m} X'_{i+m'-m} \to \prod_{i=1}^{k} X_i \times \prod_{i=k+1}^{m} X_i$$

the identity map. This completes the proof. □

Observe that Lemma 6 and Lemma 7 can be concatenated to obtain a single, coherent, extension. The variables added in Lemma 6, that run over the whole group G, will also be moving over G after the second extension provided by Lemma 7. We summarize the results of this Section in the following Proposition.

Proposition 8. *Let G be an abelian group of order n. Let $\{A, b, \mathcal{X}\}$, where A is an integer $(k \times m)$ matrix, be a non–thin restricted system with $\gcd(d_k(A), n) = 1$. There is an extension $\{A', b', \mathcal{X}'\}$ of $\{A, b, \mathcal{X}\}$ with $k' = k'(A)$ such that A' is of the form $A' = (I_{k'}|B)$, $b' = 0$ and every k' consecutive columns of A' form a unimodular matrix.*

4 Proof of Theorem 1

We complete here the proof of Theorem 1. We assume that the system is not thin, otherwise, the result holds by deleting just one element of one set.

By Lemma 4 we may assume that $m' - k' \geq 2$. Let $\epsilon > 0$ and an integer $(k \times m)$ matrix A be given. Let G be an Abelian group of order n coprime with $d_k(A)$, and let $\{A, b, \mathcal{X}\}$ be a restricted system in G. It follows from Proposition 8 that there is an extension $\{A', 0, \mathcal{X}'\}$ of $\{A, b, \mathcal{X}\}$ such that A' is a circular unimodular matrix of dimension $(k' \times m')$ with $m' - k' = m - k$ and $k' = k'(A)$. Moreover there is a subset $I_0 \subset [1, m']$ with cardinality m, a bijection $\sigma : I_0 \to [1, m]$ and maps $\phi_i : X'_i \to X_{\sigma(i)}$, $1 \leq i \leq m$ such that the map $\phi : \mathcal{X}' \to \mathcal{X}$ with $(\phi(x'))_i = \phi_{\sigma^{-1}(i)}(x'_{\sigma^{-1}(i)})$ induces a bijection between the set of solutions of $\{A', 0, \mathcal{X}'\}$ and the set of solutions of $\{A, b, \mathcal{X}\}$. In addition, $I = [1, m'] \setminus I_0$ has cardinality less than k' and $X'_i = G$ for each $i \in I$.

We apply Lemma 3 to the extension $\{A', 0, \mathcal{X}'\}$ to obtain a set $\bar{\mathcal{X}}'$ with $|\bar{X}'_i| < \epsilon n$ for all $i \in [1, m']$ such that $\{A', 0, \mathcal{X}' \setminus \bar{\mathcal{X}}'\}$ has no solution. We use the last part of Lemma 3 to ensure that $\bar{\mathcal{X}}'$ can be chosen in such a way that $\bar{X}'_i = \emptyset$ for each $i \in I = [1, m'] \setminus I_0$. This shows that $\{A, b, \mathcal{X} \setminus \phi(\bar{\mathcal{X}}')\}$ is solution free and $|(\phi(\bar{\mathcal{X}}'))_i| < \epsilon n$ for $i \in [1, m]$. This completes the proof of Theorem 1.

References

[1] Tim Austin and Terence Tao. On the testability and repair of hereditary hypergraph properties. Random Structures Algorithms, to appear.

[2] Pablo Candela. On systems of linear equations and uniform hypergraphs. manuscript, 2008.

[3] Gabor Elek and Balázs Szegedy. Limits of hypergraphs, removal and regularity lemmas. a non-standard approach. arXiv:0705.2179, 05 2007.

[4] Maozhong Fang. On the completion of a partial integral matrix to a unimodular matrix. Linear Algebra Appl., 422(1):291–294, 2007.

[5] William Timothy Gowers. Hypergraph regularity and the multidimensional Szemerédi theorem. Ann. of Math. (2), 166(3):897–946, 2007.

[6] Ben Green. A Szemerédi-type regularity lemma in abelian groups, with applications. Geom. Funct. Anal., 15(2):340–376, 2005.

[7] Yoshiyasu Ishigami. A simple regularization of graphs. arxiv:0904.4927, 2009.

[8] Daniel Král, Oriol Serra, and Lluís Vena. A combinatorial proof of the removal lemma for groups. J. Combin. Theory Ser. A, 116(4):971–978, 2009.

[9] Daniel Král, Oriol Serra, and Lluís Vena. A removal lemma for systems of linear equations over finite fields. Israel J. Math., to appear.

[10] Brendan Nagle, Vojtěch Rödl, and Mathias Schacht. The counting lemma for regular k-uniform hypergraphs. Random Structures Algorithms, 28(2):113–179, 2006.

[11] Imre Z. Ruzsa and Endre Szemerédi. Triple systems with no six points carrying three triangles. In Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, volume 18 of Colloq. Math. Soc. János Bolyai, pages 939–945. North-Holland, Amsterdam, 1978.

[12] Asaf Shapira. A proof of green's conjecture regarding the removal properties of sets of linear equations. Proc. of STOC 2009, to appear.

[13] Balázs Szegedy. The symmetry preserving removal lemma. Proc. Amer. Math. Soc., 138(2):405–408, 2010.

[14] Xingzhi Zhan. Completion of a partial integral matrix to a unimodular matrix. Linear Algebra Appl., 414(1):373–377, 2006.