Russian Math. Surveys **74**:6 1129–1131 *Uspekhi Mat. Nauk* **74**:6 167–168

DOI: https://doi.org/10.1070/RM9903

Recovery of sparse integer vectors from linear measurements

K. S. Ryutin

We consider the problem of recovering a sparse integer vector from a small number of linear measurements. This is connected with compressed sensing theory (see [1], for instance). The problem under consideration appeared as a development of studies in [2] (where the integer-valued compressed sensing problem was introduced) and [3], [4]. A very natural construction of a measurement integer matrix with good control on the absolute values of its elements that enables one to recover any sparse vector was proposed by Konyagin and Sudakov [4]. But the question of a good algorithm for recovery was not addressed. Let $\Phi = \Phi_{m\times p}$ be a matrix with elements $\phi_{ij} \in \mathbb{Z}$, where $\phi_{ij} = k_j j^{i-1} \pmod p$, $1 \leqslant j \leqslant p$, $1 \leqslant i \leqslant m$, let p be a prime number with $m \leqslant p$, and let k_j be some fixed integers with $1 \leqslant k_j < p$ (therefore, a representative of the residue class is chosen for each element of the matrix). In [4] elements were chosen so that $|\phi_{ij}| \leqslant p^{1-1/m}$.

We want to recover a vector $x \in \mathbb{Z}^p$ with s non-zero coordinates ($s \leqslant m/2$) from the given vector $y = (y_0, \dots, y_{m-1}) = \Phi x \in \mathbb{Z}^m$. Let $I = \{j_1, \dots, j_s\}$ be the support of x, and let $x_j \in \mathbb{Z}\setminus\{0\}$ with $j \in I$ be the corresponding coordinates of x. In what follows we identify indices in I with their images in the field $F = \mathbb{F}_p$. The problem under consideration is to find, from the system of equations

$$\sum_{j\in I} k_j j^l x_j = y_l, \qquad 0 \leqslant l \leqslant m-1, \tag{1}$$

the unknown set $I \subset \{1, \dots, p\}$ and the coefficients $x_j \in \mathbb{Z}$. The main difficulty is how to find the set I. We do not know the exact value of s, and the complexity of the algorithm is measured in terms of m, p, and $M = \max|x_j|$.

We will make use of some well-known algorithms for solving certain problems in finite fields. An algorithm that finds all the roots of a degree-t polynomial with simple zeros that splits over $\mathbb{F}_p$ in fewer than $tp^{1/2+o(1)}$ operations was proposed in [5]. The modification of the Berlekamp–Massey algorithm given in [6], Chap. 11, determines, after $O(s\log^{1+\varepsilon} s)$ field operations with $2s$ successive elements of a linear recurrent sequence of order s, the characteristic polynomial of the recurrence. It is known that $O(t^\omega)$ operations in a finite field F are sufficient to solve a given $t\times t$ non-homogeneous system of linear equations, where the best known upper estimate for ω is 2.4.

Theorem. *There is a deterministic algorithm that takes some vector $y = \Phi x$ as an input and, after $O(m^\omega \log_p M + m^{2+o(1)}p^{1/2+o(1)})$ arithmetical operations in the field $\mathbb{F}_p$ and $O(m^2 \log_p M)$ operations in the ring $\mathbb{Z}$, finds the unknown vector x. Moreover, the operations in $\mathbb{Z}$ are carried out with numbers not exceeding $\max\{Mp, \max_j |y_j| + mp^{1-1/m}\}$ in absolute value.*

Work supported by the Government of the Russian Federation (grant no. 14.W03.31.0031).

AMS 2010 *Mathematics Subject Classification.* Primary 15B36; Secondary 12Y05, 65F99.

We describe the scheme of the algorithm. Step by step, we find subsets $I_1 \subseteq \cdots \subseteq I_\nu \subseteq \cdots \subseteq I$ of the support of the vector x, and at the same time better and better 'p-adic' approximations for the coefficients x_j.

1. Let α be the largest power of p that divides all the coordinates of the vector y, and β the largest power of p that divides all the coordinates of x. It is clear (from the non-singularity of the corresponding matrix over F) that $\alpha = \beta$. To simplify the notation we suppose that $\alpha = \beta = 0$.

2. *The main step of the algorithm.* We consider the system (1) over the field F. Let $p(t) = \prod_{j\in I}(t-j) = \sum_{l=0}^{s} p_l t^l \in F[t]$, where the p_l are uniquely determined by the set I (and the coefficient p_s is equal to 1). It is clear that the sequence y_k is a linear recurrence with characteristic polynomial p. Namely, a simple computation gives $\sum_{l=0}^{s} p_l y_{a+l} = 0$ for any $a = 0, 1, \ldots, m-s$. It is well known that the characteristic polynomial of a minimum-length recurrence divides the characteristic polynomial of any other recurrence ([7], Chap. 8, Theorem 8.42). Hence its roots form a subset S_1 of I. Let $I_1 = S_1$. We start another iterative procedure (a part of our main step).

Procedure. There is a representation $y_l = \sum_{j\in I_1} \xi_j^{(1)} k_j j^l$ with $0 \leqslant l \leqslant m-1$ in the field F. We find the characteristic polynomial of the minimum-order recurrence for $\{y_l\}$, its roots, and the coefficients $\xi_j^{(1)} \in F$, $j \in I_1$. Note that $x_j = \xi_j^{(1)}$ for $j \in I_1$, and $x_j = 0$ for $j \in I \setminus I_1$ (all equations are in F). In fact, the vector in F^I with coordinates $x_j - \xi_j^{(1)}$ for $j \in I_1$ and x_j for $j \in I \setminus I_1$ gives a solution of a homogeneous linear system (1) with a non-singular matrix.

Consider the original system of equations in $\mathbb{Z}$. We identify $\xi_j^{(\cdot)} \in F$ with the minimum, in absolute value, representative of the residue class in $\mathbb{Z}$, that is, an integer in the set $\{0, \ldots, \pm(p-1)/2\}$, and we compute the 'error of approximation', a vector of integers $\bigl(y_l - \sum_{j\in I_1} \xi_j^{(1)} k_j j^l\bigr)_{0\leqslant l\leqslant m-1}$. If this error vector is zero, then $I_1 = I$, the vector x has been found, and the algorithm stops. Otherwise there exists an integer $\gamma_1 \geqslant 1$ which is the exponent of the highest power of p that divides all the numbers $y_l - \sum_{j\in I_1} \xi_j^{(1)} k_j j^l$, $0 \leqslant l \leqslant m-1$. We define $x_j^{(1)}$ with $j \in I$ and $y_l^{(1)}$ with $0 \leqslant l \leqslant m-1$ by the following relations: $p^{\gamma_1} x_j^{(1)} = x_j$, $j \in I \setminus I_1$; $p^{\gamma_1} x_j^1 = x_j - \xi_j^{(1)}$, $j \in I_1$; $p^{\gamma_1} y_l^{(1)} = y_l - \sum_{j\in I_1} \xi_j^{(1)} k_j j^l$, $0 \leqslant l \leqslant m-1$. Arguing as in step 1, we see that $x_j^{(1)}, y_l^{(1)} \in \mathbb{Z}$, and the solution of (1) reduces to the solution of the system

$$\sum_{j\in I} k_j j^l x_j^{(1)} = y_l^{(1)}, \qquad 0 \leqslant l \leqslant m-1. \tag{2}$$

We attempt to solve the system of equations $y_l^{(1)} = \sum_{j\in I_1} \xi_j^{(2)} k_j j^l$, $0 \leqslant l \leqslant m-1$, over F. When it is possible, we repeat the step of our Procedure. After κ_1 steps of the Procedure we obtain some system of equations in the variables $x_j^{(\kappa_1)}$ which is similar to (2) and equivalent to the original system. Moreover, it is not possible to make the (κ_1+1)st step of the Procedure.

Applying the main step of the algorithm to the system obtained after the Procedure, we find the minimal polynomial of the recurrence for $\{y_l^{(\kappa_1)}\}$; its roots form the set $S_2 \subset I$. It can happen that $I_1 \cap S_2 \neq \varnothing$. Since we have proceeded to the second step of the algorithm, we must find a new element of the support, that is,

$S_2 \setminus I_1 \neq \varnothing$. Let $I_2 = I_1 \cup S_2$. Then we start the Procedure again. It is easy to see that we will make no more than m main steps of the algorithm and no more than $O(\log_p M)$ steps of the Procedure.

The author wishes to express his deep gratitude to S.V. Konyagin for many useful discussions and for his interest in this project.

Bibliography

[1] S. Foucart and H. Rauhut, *A mathematical introduction to compressive sensing*, Appl. Numer. Harmon. Anal., Birkhäuser/Springer, New York 2013, xviii+625 pp.

[2] L. Fukshansky, D. Needell, and B. Sudakov, *Appl. Math. Comput.* **340** (2019), 31–42.

[3] С. В. Конягин, *Матем. заметки* **104**:6 (2018), 863–871; English transl., S. V. Konyagin, *Math. Notes* **104**:6 (2018), 859–865.

[4] S. V. Konyagin and B. Sudakov, *An extremal problem for integer sparse recovery*, 2019, 5 pp., arXiv: 1904.08661.

[5] J. Bourgain, S. V. Konyagin, and I. E. Shparlinski, *Math. Comp.* **84**:296 (2015), 2969–2977.

[6] R. E. Blahut, *Theory and practice of error control codes*, Addison-Wesley Publ. Co., Advanced Book Program, Reading, MA 1983, xi+500 pp.

[7] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley Publ. Co., Advanced Book Program, Reading, MA 1983, xx+755 pp.

Konstantin S. Ryutin
Lomonosov Moscow State University
E-mail: kriutin@yahoo.com

Presented by L. D. Beklemishev
Accepted 25/JUL/19
Translated by THE AUTHOR