Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 102-106*

What to do if syndroms are corrupted also?

Grigory Kabatiansky[1] kaba@iitp.ru Institute for Information Transmission Problems (IITP RAS), Moscow 127994, RUSSIA
Serge Vladuts sergevladuts@yandex.ru
Serge Vladuts, Aix-Marseille University and IITP RAS

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. We consider a discrete version of Compressed Sensing Problem when one has to find an error vector based on its syndrom for a given parity-check matrix but not all positions of the syndrom are correct. We establish analogs of some well-known bounds in coding theory and discuss how it can be applied to the original compressed sensing problem setting.

1 Introduction

The Compressed Sensing Problem [1],[2] is formulated as a problem of reconstructing of n-dimensional t-sparse vector $x \in \mathbb{R}^n$ by a few, namely, r linear measurements $s_i = (h_i, x)$, i.e., finding vector x such that $Hx^T = s$ and its Hamming weight, equals to the number of nonzero coordinates of x and denoted by $wt(x)$ or $||x||_0$, is at most t, where H is an $r \times n$ matrix, whose rows are $h_1, \ldots, h_r$, and syndrom vector $s = (s_1, \ldots, s_r)$.

Formulated in such way the problem resembles the main problem of coding theory, and it was noted for instance in [3].

We shall consider, as it is clear from our notations, matrix H as a parity-check matrix of some code. Let us note that the main achievement of Compressed Sensing is that the corresponding algorithm(s) can recover vector x even if measurements are not exact, i.e. if we know (h_i, x) with some errors $e = (e_1, \ldots, e_r)$, what is formulated as solving equation

$$s = Hx^T + e \tag{1}$$

Usual for compressed sensing assumption that vector e has relatively small Euclidean length has not much sense in discrete, especially in binary, case. Therefore we replace it on assumption that the Hamming weight of a syndrom error is not large, namely, $wt(e) \leq l$. In order to deal with parity-check matrices

[1]The work of G.Kabatiansky was supported by RFBR grants 13-07-00978 and 12-01-00905.

(as well as with linear codes) we restrict ourselves to the case when q is prime power. Let $\mathbb{F}_q$ be the finite field of q elements and F_q^n be the n-dimensional Hamming space of all q-ary vectors of length n with the Hamming distance on them $d(x,y) = |\{i : x_i \neq y_i\}| = wt(x-y)$.

Now let us consider a new problem of coding theory:
To reconstruct the vector x of the Hamming weight $wt(x) \leq t$ if all but not more than l syndrom's coordinates are correct.
The corresponding matrix H we call q -ary (t,l)-compressed sensing matrix. More formally

Definition 1 *A q -ary $r \times n$ matrix H called a (t,l)-compressed sensing (CS) matrix iff for any two distinct vectors $x, y \in \mathbb{F}_q^n$ such that $wt(x) \leq t$ and $wt(y) \leq t$ the Hamming distance between the corresponding syndroms is at least $2l+1$, i.e.*

$$d(Hx^T, Hy^T) \geq 2l+1. \tag{2}$$

Proposition 2 *A q -ary $r \times n$ matrix H is a (t,l)-CS matrix iff $wt(Hz^T) \geq 2l+1$ for any nonzero vector $z \in \mathbb{F}_q^n$ such that $wt(z) \leq 2t$.*

Remark 1. In contrary to ordinary coding theory the "redundancy size" r of CS-matrix could be larger than n.

Remark 2. In particular case $t = 1,\ l = 1$ we have got nonadaptive (or deterministic) version of famous Ulam's problem on searching with lie, see [5], and for $t = 1$ and l arbitrary - a nonadaptive version of Ulam's problem on searching with lies.

2 Upper and lower bounds for redundancy of q-ary CS matrices

The main goal of this section is to prove that for the best (t,l)-compressed sensing matrices their relative "redundancy" $\rho = r/n$ can't be too small (an analog of the ordinary Hamming bound) and to establish the counterpart upper bound for ρ (an analog of GV-bound).
Let us denote

$$V_q(n,d) = \sum_{i=0}^{i=d} C_n^i (q-1)^i = |\{x \in \mathbb{F}_q^n : wt(x) \leq d\}|$$

the volume of radius d ball in $\mathbb{F}_q^n$. Denote, as usual, by $A_q(n, 2t+1)$ the maximal possible cardinality of q-ary code correcting t errors and $A_q^{(lin)}(n; 2t+1)$ the same value taken over linear codes. Let $r_q(n,t;l)$ be the minimal redundancy r taken over all q -ary $r \times n$ (t,l)-CS matrices. Then by definitions

$$r_q(n,t;0) = n - \log_q A_q^{(lin)}(n, 2t+1)$$

Theorem 3 *(Hamming bound). For any q -ary (t,l)-CS $r \times n$-matrix*

$$A_q(r, 2l+1) \geq V_q(n,t). \tag{3}$$

Proof. The proof is obvious. According to Definition 1 the set of syndroms $\{Hx^T : wt(x) \leq t\}$ forms a code of length r capable to correct l errors, and hence the number of syndroms cannot be larger than $A_q(r, 2l+1)$. □

The r.h.s. of (3) can be rather tight approximated as $q^{nh_q(t/n)+t\log_q(q-1)}$ and instead of l.h.s. any upper bound for the cardinality of codes (see [4]) can be taken. Let us define the corresponding *relative* values: $\lambda = l/n,\ \tau = t/n$, and denote

$$\rho_q(\tau,\lambda) = \lim_{n\to\infty} r_q(n,t;l)/n.$$

Then, for instance, taking the Plotkin bound, namely, $\log_q(A_q(r, 2l+1)) \leq r - \frac{2q}{q-1}l + O(1)$ leads to the following asymptotic bound

$$\rho_q(\tau,\lambda) \geq \frac{2q}{q-1}\lambda + h_q(\tau) + \tau\log_q(q-1), \tag{4}$$

where $h_q(x) = -(x\log_q x + (1-x)\log_q(1-x))$. In the binary case it gives

$$\rho_q(\tau,\lambda) \geq 4\lambda + h_2(\tau) \tag{5}$$

On the other hand, there is the following analog of the Gilbert-Varshamov bound.

Theorem 4 *(G-V bound).*

$$r_q(n,t;l) \leq \log_q V_q(n,2t) + \log_q V_q(r,2l). \tag{6}$$

Proof. Consider random q-ary $r \times n$-matrix H which entries are taken as random independent uniformly distributed variables from $\mathbb{F}_q$. Then for any given *nonzero* vector $z \in \mathbb{F}_q^n$ its syndrom Hz^T is a random variable uniformly distributed on $\mathbb{F}_q^r$. Hence the probability that $wt(Hz^T) \leq 2l$ equals to $q^{-r}V_q(r,2l)$. And by union bound the probability that for random matrix H the Proposition 1 is not true is at most $(V_q(n,2t)-1)q^{-r}V_q(r,2l)$. □

Remark. One can use Varshamov procedure of "exausting" the space $\mathbb{F}_q^n$ of matrix H columns and then get slightly better bound, namely,

$$r_q(n,t;l) \leq \log_q V_q(n, 2t-1) + \log_q V_q(r, 2l). \tag{7}$$

Asymptotically we have (in both cases) the following lower bound on r for $2\tau < \frac{q-1}{q}, 2\lambda < \frac{q-1}{q}$

$$\rho_q(\tau,\lambda) \leq 2\log_q(q-1)(\tau+\lambda) + h_q(2\tau) + \rho(\tau,\lambda)h_q(2\lambda), \tag{8}$$

and in the binary case for $\tau < 1/4,\ \lambda < 1/4$

$$\rho(\tau,\lambda) \leq \frac{h(2\tau)}{1-h(2\lambda)} \tag{9}$$

3 Real Compressed Sensing - no small errors case and slightly beyond

First papers on Compressed Sensing contained some exclamations that this new technique (application of l_1 minimization instead of l_0) allows to recover information vector $x \in \mathbb{R}^n$ in case when not many coordinates of x were affected by errors. For instance, in [3] "one can introduce errors of arbitrary large sizes and still recover the input vector exactly by solving a convenient linear program...". To achieve such performance some special restriction on matrix H was placed, called Restricted Isometry Property (RIP), as follows

$$(1-\delta_D)||x||_2 \leq ||Hx^T||_2 \leq (1+\delta_D)||Hx||_2, \tag{10}$$

for any vector $x \in \mathbb{R}^n : ||x||_0 \leq D$, where $0 < \delta_D < 1$. The smallest possible δ_D called the isometry constant.
Then typical result looks like this (Th. 1.1 from [3])
"if $\delta_{3t} + 3\delta_{4t} < 2$ then the solution of linear programming problem is unique and equal to x"
Let us note that the condition $\delta_{3t} + 3\delta_{4t} < 2$ implies $\delta_{4t} < 2/3$ (of course, it implies that $\delta_{4t} < 1/2$, but for us enough to have $\delta_{4t} < 1$). Hence $Hx^T \neq \mathbf{0}$ for any nonzero x with $wt(x) \leq 4t$, or saying in other words, an error-correcting code (over reals) corresponding to such parity-check matrix H has the minimal distance at least $4t+1$ and can correct $2t$ errors (instead of t). So we lost twice in error-correction capability but maybe linear programming provides more easier way for decoding?
In fact, NOT, since it is well known in coding theory that such problem can

be solved rather easily (in complexity) over *any infinite field* by usage of the corresponding Reed-Solomon codes and known decoding algorithms. In case of real number or complex number fields one can use just RS code with Fourier parity-check matrix, namely, $h_{j,p} = exp(2\pi i \frac{jp}{n})$, where $p \in \{1, 2, ..., n\}$ and "roots" $j = a, a+d, a+2d, \ldots, a+(r-1)d$ for complex numbers, and "reversible" RS-matrix H for real numbers with $j \in \{-f, -f+1, \ldots, 0, 1, \ldots, f\}$ and $r = 2f+1$.
Fortunately, matrices with RIP property allow correct not only sparse errors but also additionally errors with arbitrary support but relatively small Euclidean norm. Again, RIP property is good for linear programming decoding but too strong in general. Indeed, if the following weaker property

$$\lambda_{2t}||z||_2 \leq ||Hz^T||_2, \tag{11}$$

with $\lambda_{2t} > 0$ is valid for any $z \in \mathbb{R}^n :\ ||z||_0 \leq 2t$ then the equation (1) has a unique solution for errors e such that $2||e||_2 < \lambda_{2t}||x||_2$. Let us note that for "reversible" RS-matrix H any r columns are linear independent and hence $\lambda_{2t} > 0$. Unfortunately λ_{2t} tends to zero when n grows and code rate is fixed. To find better class codes over reals is an open problem!

References

[1] D. L. Donoho, Compressed sensing, *IEEE Transactions on Information Theory*, v. 52 (4), 2006, 1289-1306.

[2] E. J. Candes, T. Tao, Near-optimal signal recovery from random projections: universal encoding strategies?, *IEEE Transactions on Information Theory*, v. 52 (12), 2006, 5406-5425.

[3] E. J. Candes, T. Tao, Decoding by linear programming, *IEEE Transactions on Information Theory*, v. 51 (12), 2005, 4203-4215.

[4] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Mathematical Library)

[5] A. Pelc, Solution of Ulam's problem on searching with a lie, *Journal of Comb. Theory*, Ser.A 44, 1987, 129-140.