Journal of Computational Mathematics, Vol.24, No.3, 2006, 357–364.

DISTURBED SPARSE LINEAR EQUATIONS OVER THE 0-1 FINITE FIELD *[1)]

Ya-xiang Yuan and Zhen-zhen Zheng
(*LSEC, ICMSEC, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100080, China*)

Dedicated to the 70th birthday of Professor Lin Qun

Abstract

In this paper, disturbed sparse linear equations over the 0-1 finite field are considered. Due to the special structure of the problem, the standard alternating coordinate method can be implemented in such a way to yield a fast and efficient algorithm. Our alternating coordinate algorithm makes use of the sparsity of the coefficient matrix and the current residuals of the equations. Some hybrid techniques such as random restarts and genetic crossovers are also applied to improve our algorithm.

Mathematics subject classification: 65L05, 65F10.
Key words: Sparse linear equation, 0-1 finite field, Alternating direction method, Random restart, Genetic hybrids.

1. Introduction

In this paper, we study the problem of solving large sparse linear equations over $GF(2)$, the field with two elements. Let $F = \{0, 1\}$, the problem can be written as

$$\begin{array}{rcl} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n & = & b_1, \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n & = & b_2, \\ \vdots & \vdots & \vdots \\ a_{m1}x_1 \oplus a_{m2}x_2 \oplus \ldots \oplus a_{mn}x_n & = & b_m, \end{array} \tag{1.1}$$

where $\oplus$ is the "exclusive or" operator over the 0-1 field, namely

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0, \tag{1.2}$$

and where $A = (a_{ij}) \in F^{m\times n}$ is a given sparse matrix, $b = (b_i) \in F^m$ is a given vector and $x = (x_i) \in F^n$ is the variable that we need to calculate, with m and n being two positive integers. Such a problem have many applications, including classification problems [14] and integer factorization problems [5, 6].

However, solving large sparse linear systems over finite fields is not easy. The most common approach to this problem is to generalize or modify the standard numerical methods for linear equations defined in $\Re^n$, such as structured Gaussian elimination, conjugate gradient, and block Lanczos algorithm (see [13, 5]). Another famous approach is due to Wiedemann, whose method uses "coordinate recurrence" and the minimum polynomial of the sub-matrices of the coefficient matrix A(see [17, 6]).

* Received March 1, 2006.
[1)] This work is partially supported by Chinese NSF grant 10231060 and the CAS Knowledge Innovation Program.

For simplicity, we denote problem (1.1) by

$$\bigoplus_{j=1}^{n} a_{ij}x_j = b_i, \qquad i = 1, ..., m\ . \tag{1.3}$$

It is quite usual for many application problems to have $m >> n$ in which case the equations (1.3) have no solution. Therefore, it is natural for us to consider the least squares problem:

$$\min_{x\in F^n} \sum_{i=1}^{m} \left(\bigoplus_{j=1}^{n} a_{ij}x_j - b_i \right)^2 . \tag{1.4}$$

If the operator $\bigoplus$ is replaced by $\sum$ in the above problem and if some simple linear constraints are added, (1.4) turns into the standard quadratic assignment problem, which has been widely studied (see [3, 4, 15, 1, 18]). The amazing success of semi-definite programming relaxations to quadratic assignment problems(for example, see[20, 2]) naturally suggests us to explore the possibilities of applying relaxations to problem (1.4). Indeed, we tried interior-point gradient methods with diagonal-scalings [19] and trust-region interior-point algorithms [7] to solve the relaxation problem to (1.4). But unfortunately, our numerical experiments show that it is difficult and time-consuming for interior point methods to find good solutions of this particular problem.

Therefore, we investigated other possible approaches to solve this difficult problem. Coming into our minds was one very simple technique: the alternating coordinate direction search method. The alternating direction search method is one of the direct methods for nonlinear optimization problems. It tries to find a minimum of a nonlinear function defined in the n dimensional space by searching along n coordinate directions in turns. The classical alternating directions methods include the pattern search method by Hooke and Jeeves [12] and Rosenbrock's method [16]. Considering the binary and sparse properties of the problem, we noticed that the basic idea of alternating directions could be implemented here very efficiently. At a typical step when we search along a coordinate direction j, all we need to do is just to compare the objective function values at two points, which can be easily done by counting the non-zero elements of the current residual vector from those indices i such that a_{ij} are non-zero.

The numerical results for the alternating coordinate search method are very encouraging, particularly for the zero residual problems, namely problems that have an exact solution. Actually our simple algorithm also works very well for disturbed problems when the sparsity is over 97 %. The disturbed systems are generated by randomly changing b, where b is the right hand side vector of a zero-residual problem. In order to improve our algorithm, we also consider random restarts and genetic hybrid techniques.

This paper is organized as follows. In the following section we present an alternating direction algorithm for sparse linear equations over finite field of two elements. Numerical results of our algorithm are given in Section 3. In Section 4 we discuss random and genetic hybrids improvement techniques and give some more computational results. Finally, some concluding remarks are given in Section 5.

2. The Alternating Direction Algorithm

Define the residual vector $r(x) \in F^m$ by

$$r_i(x) = |\bigoplus_{j=1}^{n} a_{ij}x_j - b_i| \quad (i = 1, ..., m). \tag{2.1}$$

Due to the fact that r_i is either 0 or 1, we can easily see that problem (1.4) is equivalent to

$$\min_{x\in F^n} \|r(x)\|_1. \tag{2.2}$$