组合数学在密码学中的应用之稀疏方程组的求解

江昱峰1

(1. 西安电子科技大学 计算机科学与技术学院 陕西 西安 710071)

摘要： 如今，稀疏方程组在科学和工程中经常出现。在这篇文章中，我们处理了密码分析中常见的稀疏系统。给定一个密码系统，将其转换为稀疏方程组，然后求解系统以检索密钥或明文。*Raddum*和*Semaev*提出了一种求解这种稀疏系统的新方法。事实证明，组合 *MaxMinMax* 问题在其方法的平均计算复杂度最大的情况下提供了边界。我们专注于这个 *MaxMinMax* 问题，并在有限和无限场上给出结果。

关键词： 稀疏方程组；计算复杂度；代数密码分析

# *Review* *suggestion* *to* *technical* *paper*

## *Jiang* *Yufeng*1

(1. *School* *of* *Computer* *Science* *and* *Technology*, *Xidian* *University*, *Xi*’*an* 710071, *China*)

***Abstract*:** *Nowadays* *sparse* *systems* *of* *equations* *occur* *frequently* *in* *science* *and* *engineering*. *In* *this* *contribution* *we* *deal* *with* *sparse* *system* *that* *are* *common* *in* *cryptanalysis*. *Given* *a* *cipher* *system*, *one* *converts* *it* *into* *a* *system* *of* *sparse* *equations*, *and* *then* *the* *system* *is* *solved* *to* *retrieve* *either* *a* *key* *or* *a* *plaintext*. *Raddum* *and* *Semaev* *proposed* *a* *new* *method* *for* *solving* *such* *sparse* *systems*. *It* *turns* *out* *that* *a* *combinatorial* *MaxMinMax* *problem* *provides* *bounds* *on* *the* *case* *where* *the* *average* *computational* *complexity* *of* *their* *method* *is* *maximum*. *We* *focus* *on* *this* *MaxMinMax* *problem* *and* *present* *results* *over* *finite* *and* *infinite* *fields*.

***Key*** ***Words*:** *sparse* *system* *of* *equations*；*a* *computational* *complexity*；*a* *lgebraic* *cryptanalysis*

1. **引言**

密码学是计算机科学中的一个重要分支领域，致力于保护信息的安全性和保密性。在密码学中，组合数学起着关键的作用，为密码算法的设计、分析和实现提供了理论基础和工具。

随着互联网的快速发展和信息交流的普及，保护敏感信息的安全性变得尤为重要。密码学通过使用密码算法来加密和解密数据，确保只有授权的用户能够访问和理解信息。组合数学为密码学提供了许多重要的概念和技术，如置换、排列、组合、有限域、布尔函数等。

在密码学中，组合数学的应用广泛而深入。例如，在对称密码学中，组合数学的概念被用于设计和分析流密码和块密码算法。排列和置换的概念被用于构建置换网络和置换盒，以实现数据的混淆和扩散。组合数学的组合和排列技术也被应用于密码分析，如差分分析和线性分析。

此外，组合数学在公钥密码学中也扮演着重要的角色。公钥密码学使用非对称密钥体系，其中包括公钥和私钥。组合数学中的数论和代数结构被广泛应用于公钥密码算法的设计和安全性分析。例如，基于大素数分解的RSA算法和基于椭圆曲线离散对数问题的椭圆曲线密码算法。

总之，组合数学在密码学领域的应用是不可忽视的。它为密码算法的设计、密码分析的方法以及密码协议的安全性提供了重要的数学基础。随着计算机技术的不断发展和安全需求的不断增加，组合数学在密码学中的应用将继续扩展和深化。

1. **相关工作**

稀疏对象，如稀疏矩阵和（非线性）方程的稀疏系统，在科学或工程中经常出现。目前，稀疏系统在代数密码分析中经常被研究。首先，给定一个密码系统，将其转换为方程组。其次，求解方程组以检索密钥或明文。如[1]中所指出的，该方程组将是稀疏的，因为实数系统的有效实现需要低门计数。

关于稀疏方程组求解方法的论文很多。在[2]中，人们设计了一种所谓的Gluing算法来求解有限域上的此类方程组。如果给出第一个方程的解集以及下一个方程，那么该算法就会构建解集。其中是方程总数，是在第一个方程中出现的所有未知数的集合。显然，用胶合算法找到系统所有解的复杂度取决于方程的顺序。因此，我们有兴趣找到一个能使平均复杂度最小的置换，同时也有兴趣描述最坏的情况，即平均复杂度最大的方程组。因此，Semaev在[5]中建议研究下一部分中的组合最大最小问题。

1. **原理方法**

让成为所有集合的族，其中是底层-set的子集，并且对所有成立；我们允许某些集合在中出现不止一次。那么我们定义

|  |  |
| --- | --- |
|  | (1) |

其中，最小值遍及上的所有排列，最大值遍及中的所有族。

在[3]中，作者将自己的研究局限于对所有的情况。该文表明，对于和所有，等于顶点上带有边的简单图中非琐成分的最大数目；特别是，对于，。该论文的主要结果认为是线性增长的。更确切地说，以下估计是有效的。

**定理1.1**对于所有足够大的，成立，而对于所有，成立。

后来，[5]又证明了一个渐进性更好的上界；而且，该证明是算法性的。

**定理1.2**对于所有.

作为推论，我们得到让固定不变。如果，那么对于任意的和，在中找到多项式方程系统的所有解的平均复杂度最多为。

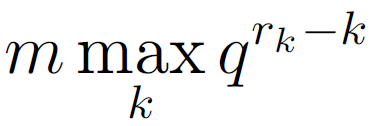
在[3]中，提出了一种解决密码分析中常见代数方程系统的新方法。这种方法与其他方法的不同之处在于，方程不是用多元多项式表示，而是用多右边线性方程组（MRHS）表示。其结果大大超越了之前使用格罗布纳基础相关算法所取得的成果。我们指出，描述高级加密标准（AES）的方程也可以用MRHS形式表示。AES可能是最常用的对称密钥密码；而在国外，经美国商务部长批准，AES成为联邦政府标准。它是第一个经美国国家安全局（NSA）批准的可公开访问的开放密码，在NSA批准的密码模块中使用时可用于处理绝密信息。

让成为上的列-向量。那么MRHS是一个系统

|  |  |
| --- | --- |
|  | (2) |

其中，是大小为、秩为的矩阵，是长度为的列向量。如果满足(2)中的所有结论，那么它就是(2)的解。解此类方程的方法在[4]中也有介绍。

我们这篇论文的主要目标之一是求解(2)的复杂度的渐近极限。正如塞马耶夫所指出的，可以通过研究(2)所描述的组合问题的一般化来获得这种界限。这个想法基于以下陈述，它可以用组合术语来表述给定的密码问题。让表示中所有行向量的秩。

**定理1.3**假设(2)中的右侧列向量是上每个变量的阶数为的均匀随机多项式的零点（换句话说，每个特定列向量以概率独立出现）。那么求解(2)的平均复杂度最多为

因此，与原问题一样，解法的复杂度取决于矩阵的秩。因此，问题的复杂度实际上是对(1)中定义的函数的概括，即用属于第一个矩阵的向量的秩来代替第一个集合的大小。形式上，让成为-维向量空间、over或真实数字空间中所有对所有的限制条件下，所有向量集的集合族。我们设

|  |  |
| --- | --- |
|  | (3) |

其中，最小值遍及上的所有排列，最大值遍及中的所有族。

虽然函数和的定义相似，但它们的行为却大相径庭。

显然，是一个微不足道的上界。对于某些向量空间，这个界限是可以达到的。对于真实数字的-维空间，这个约束的严密性来自这样一个事实：包含无穷多个向量，而其中任何都是独立的。

我们现在重点讨论对问题的原始密码学设置非常重要的有限域。如上所述，对所有都成立。事实证明，即使是的情况，对于大多数向量空间也是一个挑战。令人惊讶的是，利用里德-所罗门码，即使对某些有限域也能达到一个较小的上界。

**定理1.4**设是有限域，其中。那么对于任何，我们都有。

最后，我们把重点放在二进制域上，这是加密应用中最重要的域。我们从上限开始。

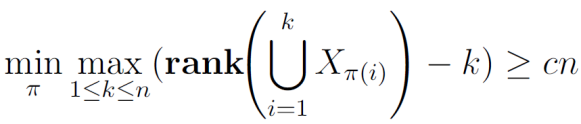
**定理1.5**存在一个绝对常数，使得。

至于下限，我们首先根据线性二进制码大小的吉尔伯特-瓦尔沙莫夫类型渐近下限提出一个线性下限。

**定理1.6**对于所有足够大的，有。

目前，我们还没有关于函数的渐近增长率的猜想。为了说明这个问题的难度，我们提出了一个族，表明即使通过一个非常特殊的系统，也可以得到的线性下限。

**定理1.7**对于足够大的，存在一个正常数和一个二进制向量族，其中对于所有，且包含一个单位向量和一个恰好有两个非零坐标的向量，使得



其中最小值遍及上的所有排列。

1. **结果与讨论**

结果见上。本文所用原理方法的优点是具有鲁棒性、可转移性，合理可行，不过也存在一定的局限性、理想化等问题需要进一步改进。

1. **致谢**

感谢NogaAlon对概率方法的讨论，这些讨论改进了定理1.1中的下界。

**参考文献：**

[1] *N. T. Courtois, and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations" in Advances of Cryptology, Asiacrypt* 2002*, LNCS* 2501*, Springer,* 2002*,* 267-287*.*

[2] *P. Horak and Zs. Tuza, Speeding up deciphering by hypergraph ordering, Designs, Codes and Cryptography* 75 (2015), 175 185*.*

[3] *H. Raddum, and I. Semaev, Solving multiple right hand side equations, Designs, Codes and Cryptography* 49 (2008)*,* 147-160*.*

[4] *I. Semaev, On solving sparse algebraic equations over finite fields, Designs, Codes and Cryptography* 49 (2008), 47-60*.*

[5] *I. Semaev, MaxMinMax problem and sparse equations over finite fields, Desings, Codes and Cryptography, DOI* 10.1007/s10623-015-0058-6*.*