有限域上 Galois 型非线性移位寄存器的能观性

高哲[1]，冯俊娥[1]，于永渊[1]，崔彦君[2]
[1]山东大学数学学院，中国济南市，250100
[2]明尼苏达大学双城分校计算机科学与工程系，美国明尼苏达州，55455

摘要：能观性可以确保任何两个不同初始状态都可以由它们的输出序列唯一确定，因此流密码必须避免不可观的非线性反馈移位寄存器，以防止等效密钥的出现。本文讨论了有限域上Galois型非线性反馈移位寄存器的能观性。通过半张量积，Galois型非线性反馈移位寄存器可被视为逻辑网络。本文介绍了状态转移矩阵的向量形式，据此提出一个充分必要条件以及判定一般Galois型非线性反馈移位寄存器能观性的算法。此外，本文定义了一个新的能观性矩阵，通过该矩阵可推导出计算复杂度较低的矩阵方法。此外，研究两种特殊类型的Galois型非线性反馈移位寄存器的能观性：全长Galois型非线性反馈移位寄存器和非奇异Galois型非线性反馈移位寄存器。提出两种方法确定这两种特殊类型的非线性反馈移位寄存器的能观性，并提供一些数值示例支持这些结果。

关键词：能观性；非线性反馈移位寄存器（NFSRs）；Galois型非线性反馈移位寄存器；半张量积；有限域；逻辑网络

https://doi.org/10.1631/FITEE.2200228