On Some Algebraic Structures in the AES Round Function

A. M. Youssef and S. E. Tavares

Department of Electrical and Computer Engineering
Queen's University
Kingston, Ontario K7L 3N6, CANADA
{amr_y,tavares}@ee.queensu.ca

Abstract. In this paper, we show that all the coordinate functions of the Advanced Encryption Standard (AES) round function are equivalent under an affine transformation of the input to the round function. In other words, let f_i and f_j be any two distinct output coordinates of the AES round function, then there exists a nonsingular matrix A_{ji} over $GF(2)$ such that $f_j(A_{ji}x) + b_{ji} = f_i(x), b_{ji} \in GF(2)$. We also show that such linear relations will always exist if the Rijndael s-box is replaced by any bijective monomial over $GF(2^8)$.

Key words. Cryptography, AES, Rijndael, Finite fields, Boolean functions

1 Introduction

Rijndael [2], [3] is an iterated block cipher that supports key and block lengths of 128 to 256 bits in steps of 32 bits. Rijndael versions with a block length of 128 bits, and key lengths of 128,192 and 256 bits have been adopted as the Advanced Encryption Standard (AES) [4]. The main cryptographic criteria in the design of Rijndael have been its resistance against differential [1] and linear cryptanalysis [11]. This motivated the designers to choose an s-box which is optimized against these two attacks. In particular the designers decided to base their s-box construction on the inversion mapping [14]

$$f(x) = x^{-1}, x \in GF(2^8).$$

Because this inverse mapping has a very simple algebraic expression that may enable some attacks such as the interpolation attacks [8], [9], this mapping was modified in such a way that doesn't modify its resistance towards both linear and differential cryptanalysis while the overall s-box description becomes complex in $GF(2^8)$. This was achieved by adding a bitwise affine transformation after the inverse mapping. Let $a(x)$ denote the finite field polynomial representation of the s-box output, then the finite field polynomial representation of the output of this affine mapping is given by

$$b(x) = (x^7 + x^6 + x^2 + x) + a(x)(x^7 + x^6 + x^5 + x^4 + 1) \bmod (x^8 + 1). \quad (1)$$

Like many other block ciphers, the Rijndael s-boxes provide the only source of nonlinearity to the Rijndael round function, and hence to the overall algorithm. Weaknesses discovered with these mappings may have some consequences for the security of the overall cipher. Even before the AES proposal, Gong and Golomb [7] introduced a new criterion for s-box design. By showing that many DES-like ciphers can be viewed as a nonlinear feedback shift register with input, Gong and Golomb proposed that s-boxes should not be approximated by a bijective monomial. The reason is that, for $gcd(c, 2^n - 1) = 1$, the trace functions $Tr(\zeta_j x^c)$ and $Tr(\lambda x), x \in GF(2^n)$, are both m-sequences with the same linear span.

Several other concerns were raised about the algebraic structure of the AES [5] [13]. Recently, J. Fuller and W. Millan [6] showed, using a heuristic search technique, that all the coordinate functions of the Rijndael s-box can be mapped to each other using an affine transformation of the input variables. In this paper we extend their result by using the algebraic properties of the Rijndael s-box. In particular, we show that all the coordinate functions of the Rijndael round function are equivalent under an affine transformation of the input to the round function. In other words, let $f_i(x)$ and $f_j(x)$ be any two distinct outputs of the Rijndael round function, then there exists a nonsingular matrix A_{ji} over $GF(2)$ such that $f_j(A_{ji}x) + b_{ji} = f_i(x), b_{ji} \in GF(2)$. We also show that such linear relations will always exist if the Rijndael s-box is replaced by any bijective monomial over $GF(2^8)$.

2 Rijdael Round Transformation

In this section we briefly describe a typical round function of the 128-bit version of Rijdael. The first and last rounds have slightly different form but our analysis procedure remains the same. The input to the AES round function can be viewed as a rectangular array of bytes. The AES defines a round in terms of the following three transformations: Byte substitution (ByteSub) , Shift row (ShiftRow) and Mix columns (MixColumns). After performing theses three operations, the round keys are XORed with the output of the round functions. According to the AES specifications, the intermediate cipher result is called a state which can be represented by a rectangular array. The round function operations are defined on theses states. The ByteSub is obtained by first taking the multiplicative inverse in $GF(2^8)$ using the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. Then we apply the affine transformation defined by equation (1) above. In the ShiftRow transformation, the rows of the State are cyclically shifted over different offsets depending on the cipher block length. For the 128 bit version, row i is cyclically shifted by i bytes, $i = 0, 1, 2, 3$. In the MixColumn transformation, the columns of the state are considered as polynomials over $GF(2^8)$ and multiplied modulo $x^4 + 1$ with the polynomial $c(x) = 3x^3 + x^2 + x + 2$. For full details on the round transformation the reader is referred to [2], [4].

3 Algebraic Preliminaries

In this section we present some algebraic preliminaries required to prove our result. The reader is referred to [10], [12] for the theory of finite fields.

Let $\{\alpha_0 \cdots \alpha_{n-1}\}$ be any basis of $GF(2^n)$ over $GF(2)$ and let $\{\beta_0 \cdots \beta_{n-1}\}$ be the corresponding dual basis. Let $f(x_0, \cdots, x_{n-1}) = (f_0(x), \cdots, f_{n-1}(x))$ be a permutation over $GF(2)^n$, then $F(X) = \sum_{i=0}^{n-1} \alpha_i f_i(x_0, \cdots, x_{n-1})$ is also a bijective mapping over $GF(2^n)$. Each output coordinate of $f(x)$ can be expressed as

$$f_i(x) = Tr(F(X)\beta_i),$$

where $X = \sum x_i \alpha^i$. We will denote this one-to-one correspondence by $f \longleftrightarrow F$.

Example 1. Let $n = 4$ and let $GF(2^4)$ be defined by the primitive polynomial $p(x) = x^4 + x + 1$. Let α be a root of $p(x)$. Then $\{\alpha_0, \alpha_1, \alpha_2, \alpha_3\} = \{1, \alpha, \alpha^2, \alpha^3\}$ is a (polynomial) basis of $GF(2^4)$ over $GF(2)$. The dual basis $\{\beta_0, \beta_1, \beta_2, \beta_3\}$ is given by [12]

$$\beta_j = \sum_{k=0}^{3} b_{kj}\alpha_k,$$

where $B = [b_{ij}] = A^{-1}$, $A = [a_{ij}]$ and $a_{ij} = Tr(\alpha_i \alpha_j)$. Thus we have

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad B = A^{-1} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Hence we have $\{\beta_0, \beta_1, \beta_2, \beta_3\} = \{1 + \alpha, \alpha^2, \alpha, 1\} = \{\alpha^{14}, \alpha^2, \alpha, 1\}$. Let $F(x) = Tr(x^{-1})$. For any $X \in GF(2^4)$, we write $x = x_0 + x_1\alpha + x_2\alpha^2$. Then

$$\begin{aligned} f_0(x) &= Tr(\beta_0 x^{-1}) = Tr(\alpha^{14} x^{-1}), \\ f_1(x) &= Tr(\beta_1 x^{-1}) = Tr(\alpha^2 x^{-1}), \\ f_2(x) &= Tr(\beta_2 x^{-1}) = Tr(\alpha x^{-1}), \\ f_3(x) &= Tr(\beta_3 x^{-1}) = Tr(x^{-1}). \end{aligned}$$

Lemma 1. *Let $F(X) = X^d$, $gcd(d, 2^{n-1} = 1)$, be a bijective monomial over $GF(2^n)$. Let $G(X) = L(F(X))$ be the function obtained by applying an invertible linear transformation L to the output coordinates of F. Then the output coordinates of $g \longleftrightarrow G$ can be mapped to each other using an affine transformation in the form $g_i(x) = g_j(A_{ji}x)$.*

Proof. Each output coordinate of $f(x)$ can be expressed as

$$f_i(x) = Tr(X^d \gamma_i), \gamma_i \in GF(2^n).$$

Thus every coordinate of $g(x)$ can be expressed as

$$g_i(x) = \sum_{i=0}^{n-1} b_i Tr(X^d \gamma_i), b_i \in GF(2).$$

From the linearity of the trace function and by noting that $Tr(b_i x) = b_i Tr(x)$ for $b_i \in GF(2)$, then

$$g_i(x) = Tr(X^d \sum_{i=0}^{n-1} \gamma_i b_i) = Tr(X^d \theta_i),$$

where $\theta = \sum_{i=0}^{n-1} \gamma_i b_i$. Hence we have

$$g_i(\theta_i^{-1/d} \theta_j^{1/d} X) = Tr(\theta_j X^d) = g_j(X).$$

The lemma follows by noting that the transformation $X \rightarrow \theta X$ over $GF(2^n)$ corresponds to a linear transformation over $GF(2)^n$.

Example 2. For the function in example 1, to transform f_1 into f_3 we use the transform $x \rightarrow \alpha^2 x$, i.e.,

$$\begin{aligned} x_0 + \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3 \rightarrow \alpha^2 (x_0 + \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3) \bmod p(x) \\ = \; x_2 + (x_2 + x_3)\alpha + (x_0 + x_3)\alpha^2 + x_1 \alpha^3 \end{aligned}$$

Thus the linear transformation we use is given by

$$\begin{bmatrix} x_0' \\ x_1' \\ x_2' \\ x_3' \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}.$$

4 Equivalence between the AES s-box coordinates

In this section we we demonstrate the affine relation between the coordinate functions of the Rijndael s-box. We construct the finite field $GF(2^8)$ using the same irreducible polynomial in the AES specifications, namely $p(x) = x^8 + x^4 + x^3 + x + 1$. Let $\beta = 1 + \alpha$ where α is a root of $p(x)$. Using the same computation step as in Example (1), the co-ordinate functions of the Rijndael s-box is given by

$$\begin{aligned} f_0(x) &= Tr(\beta^{166} x^{-1}) + 1, \\ f_1(x) &= Tr(\beta^{53} x^{-1}) + 1, \\ f_2(x) &= Tr(\beta^{36} x^{-1}), \\ f_3(x) &= Tr(\beta^{11} x^{-1}), \\ f_4(x) &= Tr(\beta^{72} x^{-1}), \\ f_5(x) &= Tr(\beta^{76} x^{-1}) + 1, \\ f_6(x) &= Tr(\beta^{51} x^{-1}) + 1, \\ f_7(x) &= Tr(\beta^{26} x^{-1}). \end{aligned}$$

Now suppose that we want to transform f_0 into f_1, we use the transformation $x \rightarrow \beta^{(166-53) \bmod 255} x = \beta^{113} x$. Thus we have

$$\begin{aligned} (x_0 + x_1\alpha + \cdots + x_7\alpha^7) \rightarrow (x_0 + x_1\alpha + \cdots x_7\alpha^7)(1+\alpha)^{113} \bmod p(x) = \\ (x_0 + x_4 + x_5) + (x_1 + x_4 + x_6)\alpha + (x_2 + x_5 + x_7)\alpha^2 + \\ (x_0 + x_3 + x_4 + x_5 + x_6)\alpha^3 + (x_0 + x_1 + x_6 + x_7)\alpha^4 + \\ (x_1 + x_2 + x_7)\alpha^5 + (x_2 + x_3)\alpha^6 + (x_3 + x_4)\alpha^7 \end{aligned}$$

which corresponds to the linear transformation

$$\begin{bmatrix} x'_0 \\ x'_1 \\ x'_2 \\ x'_3 \\ x'_4 \\ x'_5 \\ x'_6 \\ x'_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,0\,0 \\ 0\,1\,0\,0\,1\,0\,1\,0 \\ 0\,0\,1\,0\,0\,1\,0\,1 \\ 1\,0\,0\,1\,1\,1\,1\,0 \\ 1\,1\,0\,0\,0\,0\,1\,1 \\ 0\,1\,1\,0\,0\,0\,0\,1 \\ 0\,0\,1\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1\,0\,0\,0 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}$$

5 Equivalence between the AES round function coordinates

In this section we we demonstrate the affine relation between the coordinate functions of the Rijndael round function. Here we consider the 128 bit version. The same technique can be used for the other versions of the cipher. We do not use the standard AES way of representing the input to the round function as a rectangular array. Let X_i denote the input to the i^{th} s-box of the round function, then we simply view the input to the round function as a column vector. Careful examination of the ShiftRow and MixColumn operations reveals that every output byte of the round function depends only on 4 input bytes of the 16 input bytes of the round function. In particular if we let Y_i denote the i^{th} output byte of the round function, then we have

$$\begin{array}{c} Y_0,\ Y_1,\ Y_2,\ Y_3 \text{ depends only on } X_0, X_5, X_{10}, X_{15}, \\ Y_4,\ Y_5,\ Y_6,\ Y_7 \text{ depends only on } X_3, X_4, X_9, X_{14}, \\ Y_8,\ Y_9,\ Y_{10}, Y_{11} \text{ depends only on } X_2, X_7, X_8, X_{13}, \\ Y_{12}, Y_{13}, Y_{14}, Y_{15} \text{ depends only on } X_1, X_6, X_{11}, X_{12}. \end{array}$$

From the description of the round function, it is clear that the byte structure is respected throughout all three operations of the round function. Combining these observations with the fact that both the ShiftRow and MixColumns transformations are linear operations, we can easily use the Lagrange interpolation to evaluate the exact form of dependency of the output of the round function on its inputs.

Again, let $GF(2^8)$ be defined by the the irreducible polynomial defining $p(x) = x^8 + x^4 + x^3 + x + 1$. Let $\beta = 1 + \alpha$ where α is a root of $p(x)$. The 128 output coordinates of the round functions are given in Appendix I. Now we give an illustrative example for how to find the transformation matrix used to map one coordinate function to another.

Example 3. To transform the coordinate function

$$f_0 = Tr(\beta^{26} X_0^{-1}) + Tr(\beta^{154} X_5^{-1}) + Tr(\beta^{166} X_{10}^{-1}) + Tr(\beta^{166} X_{15}^{-1}) + 1$$

into

$$f_{31} = Tr(\beta^{26} X_0^{-1}) + Tr(\beta^{26} X_5^{-1}) + Tr(\beta^{51} X_{10}^{-1}) + Tr(\beta^{27} X_{15}^{-1})$$

we use the transformation

$$
\begin{aligned}
X_5 \quad &\rightarrow \beta^{127} X_5 \\
(x_0 + x_1\alpha + \cdots + x_7\alpha^7) &\rightarrow \\
&\quad (x_1 + x_3 + x_5 + x_6 + x_7) + \\
&\quad (x_1 + x_2 + x_3 + x_4 + x_5)\alpha + \\
&\quad (x_2 + x_3 + x_4 + x_5 + x_6)\alpha^2 + \\
&\quad (x_1 + x_4)\alpha^3 + \\
&\quad (x_1 + x_2 + x_3 + x_6 + x_7)\alpha^4 + \\
&\quad (x_0 + x_2 + x_3 + x_4 + x_7)\alpha^5 + \\
&\quad (x_1 + x_3 + x_4 + x_5)\alpha^6 + \\
&\quad (x_0 + x_2 + x_4 + x_5 + x_6)\alpha^7.
\end{aligned}
$$

$$
\begin{aligned}
X_{10} \quad &\rightarrow \beta^{127} X_{10} \\
(x_0 + x_1\alpha + \cdots + x_7\alpha^7) &\rightarrow \\
&\quad (x_2 + x_3 + x_3 + x_4 + x_7) + \\
&\quad (x_0 + x_2 + x_5 + x_7)\alpha + \\
&\quad (x_1 + x_2 + x_6)\alpha^2 + \\
&\quad (x_0 + x_1 + x_4)\alpha^3 + \\
&\quad (x_0 + x_3 + x_4 + x_5 + x_7)\alpha^4 + \\
&\quad (x_0 + x_1 + x_4 + x_5 + x_6)\alpha^5 + \\
&\quad (x_0 + x_1 + x_2 + x_5 + x_6 + x_7)\alpha^6 + \\
&\quad (x_0 + x_1 + x_2 + x_3 + x_6 + x_7)\alpha^7.
\end{aligned}
$$

$$
\begin{aligned}
X_{15} \quad &\rightarrow \beta^{127} X_{15} \\
(x_0 + x_1\alpha + \cdots + x_7\alpha^7) &\rightarrow \\
&\quad (x_0 + x_1 + x_5 + x_7) + \\
&\quad (x_0 + x_2 + x_5 + x_6 + x_7)\alpha + \\
&\quad (x_0 + x_1 + x_3 + x_6 + x_7)\alpha^2 + \\
&\quad (x_2 + x_4 + x_5)\alpha^3 + \\
&\quad (x_1 + x_2 + x_6 + x_7)\alpha^4 + \\
&\quad (x_2 + x_4 + x_7)\alpha^5 + \\
&\quad (x_3 + x_5)\alpha^6 + \\
&\quad (x_0 + x_4 + x_6)\alpha^7.
\end{aligned}
$$

The matrix $A_{31,0}$ is given in appendix II.

It is clear that replacing the s-box with any other monomial over $GF(2^8)$ will not change the form of dependency of the output of the round function on its inputs because we still can represent the component functions of the s-box as $Tr(\theta x^d)$. For all these monomials, we will have similar expressions as in appendix I except that the coefficients inside the trace term will be different. Thus a similar equivalence relation will still hold between the coordinates of the the round function.

6 Conclusions

We showed that all the output coordinates of the AES round function are in the same affine equivalence class. Although we were not able to utilize this observation to attack the AES cipher, this observation may raise some concerns regarding the highly structured algebraic properties of the AES round function. The implication of this result on the cryptanalysis on the AES remains an open problem.

References

1. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.
2. J. Daemen, V. Rijmen, *The Block Cipher Rijndael*, Springer-Verlag, ISBN 3-540-42580-2.
3. J. Daemen, V. Rijmen, *The Block Cipher Rijndael*, Proc. of the third international conference on smart card research and applications, CARDIS'98, LNCS 1820, pp. 277-284, 2000.
4. Federal Information Processing Standards Publication (FIPS 197) *Advanced Encryption Standard (AES)* , Nov. 26, 2001
5. N. Ferguson, R. Schroeppel, and D. Whiting, *A Simple Algebraic Representation of Rijndael*, Proc. of the 8th international workshop on Selected Areas in Cryptography (SAC'2001), LNCS 2259, p. 103-111, 2001.
6. J. Fuller and W. Millan, *On Linear Redundancy in the AES S-Box*, preprint available at http://eprint.iacr.org, August, 2002
7. G. Gong and S. W. Golomb, *Transform Domain Analysis of DES*, IEEE transactions on Information Theory. Vol. IT-45, no. 6, pp. 2065-2073, September, 1999.
8. T. Jakobsen and L. Knudsen, *The Interpolation Attack on Block Ciphers, LNCS 1267*, Fast Software Encryption, pp. 28-40. 1997.
9. T. Jakobsen, *Cryptanalysis of Block Ciphers with Probabilistic Non-linear Relations of Low degree*, Proceedings of Crypto'99, LNCS 1462, pp. 213-222, 1999.
10. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983.
11. M. Matsui, *Linear Cryptanalysis Method for DES Cipher* Advances in Cryptology, Proceedings of Eurocrypt'93, LNCS 765, pp. 386-397, Springer-Verlag, 1994.
12. R. J. McEliece, *Finite fields for Computer Scientists and Engineers* , Kluwer Academic Publishers, Dordrecht, 1987.
13. S. Murphy and M.J.B. Robshaw, *Essential Algebraic Structure Within the AES*, To appear in Proc. of Crypto 2002.
14. K. Nyberg, *Differentially Uniform Mappings for Cryptography*, Proceedings of Eurocrypt'93, LNCS 765, Springer-Verlag, pp. 55-64, 1994,

7 Appendix I Trace Representation of the AES round function coordinates

$$
\begin{aligned}
f0 &= Tr(\beta^{26}X_0^{-1}) + Tr(\beta^{154}X_5^{-1}) + Tr(\beta^{166}X_{10}^{-1}) + Tr(\beta^{166}X_{15}^{-1}) + 1\\
f1 &= Tr(\beta^{154}X_0^{-1}) + Tr(\beta^{100}X_5^{-1}) + Tr(\beta^{53}X_{10}^{-1}) + Tr(\beta^{53}X_{15}^{-1}) + 1\\
f2 &= Tr(\beta^{53}X_0^{-1}) + Tr(\beta^{104}X_5^{-1}) + Tr(\beta^{36}X_{10}^{-1}) + Tr(\beta^{36}X_{15}^{-1}) + 0\\
f3 &= Tr(\beta^{47}X_0^{-1}) + Tr(\beta^{236}X_5^{-1}) + Tr(\beta^{11}X_{10}^{-1}) + Tr(\beta^{11}X_{15}^{-1}) + 0\\
f4 &= Tr(\beta^{44}X_0^{-1}) + Tr(\beta^{237}X_5^{-1}) + Tr(\beta^{72}X_{10}^{-1}) + Tr(\beta^{72}X_{15}^{-1}) + 0\\
f5 &= Tr(\beta^{72}X_0^{-1}) + Tr(\beta^{172}X_5^{-1}) + Tr(\beta^{76}X_{10}^{-1}) + Tr(\beta^{76}X_{15}^{-1}) + 1\\
f6 &= Tr(\beta^{76}X_0^{-1}) + Tr(\beta^{52}X_5^{-1}) + Tr(\beta^{51}X_{10}^{-1}) + Tr(\beta^{51}X_{15}^{-1}) + 1\\
f7 &= Tr(\beta^{51}X_0^{-1}) + Tr(\beta^{27}X_5^{-1}) + Tr(\beta^{26}X_{10}^{-1}) + Tr(\beta^{26}X_{15}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f_8 &= Tr(\beta^{166}X_0^{-1}) + Tr(\beta^{26}X_5^{-1}) + Tr(\beta^{154}X_{10}^{-1}) + Tr(\beta^{166}X_{15}^{-1}) + 1\\
f_9 &= Tr(\beta^{53}X_0^{-1}) + Tr(\beta^{154}X_5^{-1}) + Tr(\beta^{100}X_{10}^{-1}) + Tr(\beta^{53}X_{15}^{-1}) + 1\\
f_10 &= Tr(\beta^{36}X_0^{-1}) + Tr(\beta^{53}X_5^{-1}) + Tr(\beta^{104}X_{10}^{-1}) + Tr(\beta^{36}X_{15}^{-1}) + 0\\
f11 &= Tr(\beta^{11}X_0^{-1}) + Tr(\beta^{47}X_5^{-1}) + Tr(\beta^{236}X_{10}^{-1}) + Tr(\beta^{11}X_{15}^{-1}) + 0\\
f12 &= Tr(\beta^{72}X_0^{-1}) + Tr(\beta^{44}X_5^{-1}) + Tr(\beta^{237}X_{10}^{-1}) + Tr(\beta^{72}X_{15}^{-1}) + 0\\
f13 &= Tr(\beta^{76}X_0^{-1}) + Tr(\beta^{72}X_5^{-1}) + Tr(\beta^{172}X_{10}^{-1}) + Tr(\beta^{76}X_{15}^{-1}) + 1\\
f14 &= Tr(\beta^{51}X_0^{-1}) + Tr(\beta^{76}X_5^{-1}) + Tr(\beta^{52}X_{10}^{-1}) + Tr(\beta^{51}X_{15}^{-1}) + 1\\
f15 &= Tr(\beta^{26}X_0^{-1}) + Tr(\beta^{51}X_5^{-1}) + Tr(\beta^{27}X_{10}^{-1}) + Tr(\beta^{26}X_{15}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f16 &= Tr(\beta^{166}X_0^{-1}) + Tr(\beta^{166}X_5^{-1}) + Tr(\beta^{26}X_{10}^{-1}) + Tr(\beta^{154}X_{15}^{-1}) + 1\\
f17 &= Tr(\beta^{53}X_0^{-1}) + Tr(\beta^{53}X_5^{-1}) + Tr(\beta^{154}X_{10}^{-1}) + Tr(\beta^{100}X_{15}^{-1}) + 1\\
f18 &= Tr(\beta^{36}X_0^{-1}) + Tr(\beta^{36}X_5^{-1}) + Tr(\beta^{53}X_{10}^{-1}) + Tr(\beta^{104}X_{15}^{-1}) + 0\\
f19 &= Tr(\beta^{11}X_0^{-1}) + Tr(\beta^{11}X_5^{-1}) + Tr(\beta^{47}X_{10}^{-1}) + Tr(\beta^{236}X_{15}^{-1}) + 0\\
f20 &= Tr(\beta^{72}X_0^{-1}) + Tr(\beta^{72}X_5^{-1}) + Tr(\beta^{44}X_{10}^{-1}) + Tr(\beta^{237}X_{15}^{-1}) + 0\\
f21 &= Tr(\beta^{76}X_0^{-1}) + Tr(\beta^{76}X_5^{-1}) + Tr(\beta^{72}X_{10}^{-1}) + Tr(\beta^{172}X_{15}^{-1}) + 1\\
f22 &= Tr(\beta^{51}X_0^{-1}) + Tr(\beta^{51}X_5^{-1}) + Tr(\beta^{76}X_{10}^{-1}) + Tr(\beta^{52}X_{15}^{-1}) + 1\\
f23 &= Tr(\beta^{26}X_0^{-1}) + Tr(\beta^{26}X_5^{-1}) + Tr(\beta^{51}X_{10}^{-1}) + Tr(\beta^{27}X_{15}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f24 &= Tr(\beta^{166}X_0^{-1}) + Tr(\beta^{166}X_5^{-1}) + Tr(\beta^{26X_{10}^{-1}}) + Tr(\beta^{154}X_{15}^{-1}) + 1\\
f25 &= Tr(\beta^{53}X_0^{-1}) + Tr(\beta^{53}X_5^{-1}) + Tr(\beta^{154}X_{10}^{-1}) + Tr(\beta^{100}X_{15}^{-1}) + 1\\
f26 &= Tr(\beta^{36}X_0^{-1}) + Tr(\beta^{36}X_5^{-1}) + Tr(\beta^{53}X_{10}^{-1}) + Tr(\beta^{104}X_{15}) + 0\\
f27 &= Tr(\beta^{11}X_0^{-1}) + Tr(\beta^{11}X_5^{-1}) + Tr(\beta^{47}X_{10}^{-1}) + Tr(\beta^{236}X_{15}) + 0\\
f28 &= Tr(\beta^{72}X_0^{-1}) + Tr(\beta^{72}X_5^{-1}) + Tr(\beta^{44}X_{10}^{-1}) + Tr(\beta^{237}X_{15}) + 0\\
f29 &= Tr(\beta^{76}X_0^{-1}) + Tr(\beta^{76}X_5^{-1}) + Tr(\beta^{72}X_{10}^{-1}) + Tr(\beta^{172}X_{15}) + 1\\
f30 &= Tr(\beta^{51}X_0^{-1}) + Tr(\beta^{51}X_5^{-1}) + Tr(\beta^{76}X_{10}^{-1}) + Tr(\beta^{52}X_{15}) + 1\\
f31 &= Tr(\beta^{26}X_0^{-1}) + Tr(\beta^{26}X_5^{-1}) + Tr(\beta^{51}X_{10}^{-1}) + Tr(\beta^{27}X_{15}) + 0
\end{aligned}
$$

$$f32 = Tr(\beta^{166}X_3^{-1}) + Tr(\beta^{26}X_4^{-1}) + Tr(\beta^{154}X_9^{-1}) + Tr(\beta^{166}X_{14}^{-1}) + 1$$
$$f33 = Tr(\beta^{53}X_3^{-1}) + Tr(\beta^{154}X_4^{-1}) + Tr(\beta^{100}X_9^{-1}) + Tr(\beta^{53}X_{14}^{-1}) + 1$$
$$f34 = Tr(\beta^{36}X_3^{-1}) + Tr(\beta^{53}X_4^{-1}) + Tr(\beta^{104}X_9^{-1}) + Tr(\beta^{36}X_{14}^{-1}) + 0$$
$$f35 = Tr(\beta^{11}X_3^{-1}) + Tr(\beta^{47}X_4^{-1}) + Tr(\beta^{236}X_9^{-1}) + Tr(\beta^{11}X_{14}^{-1}) + 0$$
$$f36 = Tr(\beta^{72}X_3^{-1}) + Tr(\beta^{44}X_4^{-1}) + Tr(\beta^{237}X_9^{-1}) + Tr(\beta^{72}X_{14}^{-1}) + 0$$
$$f37 = Tr(\beta^{76}X_3^{-1}) + Tr(\beta^{72}X_4^{-1}) + Tr(\beta^{172}X_9^{-1}) + Tr(\beta^{76}X_{14}^{-1}) + 1$$
$$f38 = Tr(\beta^{51}X_3^{-1}) + Tr(\beta^{76}X_4^{-1}) + Tr(\beta^{52}X_9^{-1}) + Tr(\beta^{51}X_{14}^{-1}) + 1$$
$$f39 = Tr(\beta^{26}X_3^{-1}) + Tr(\beta^{51}X_4^{-1}) + Tr(\beta^{27}X_9^{-1}) + Tr(\beta^{26}X_{14}^{-1}) + 0$$

$$f40 = Tr(\beta^{166}X_3^{-1}) + Tr(\beta^{166}X_4^{-1}) + Tr(\beta^{26}X_9^{-1}) + Tr(\beta^{154}X_{14}^{-1}) + 1$$
$$f41 = Tr(\beta^{53}X_3^{-1}) + Tr(\beta^{53}X_4^{-1}) + Tr(\beta^{154}X_9^{-1}) + Tr(\beta^{100}X_{14}^{-1}) + 1$$
$$f42 = Tr(\beta^{36}X_3^{-1}) + Tr(\beta^{36}X_4^{-1}) + Tr(\beta^{53}X_9^{-1}) + Tr(\beta^{104}X_{14}^{-1}) + 0$$
$$f43 = Tr(\beta^{11}X_3^{-1}) + Tr(\beta^{11}X_4^{-1}) + Tr(\beta^{47}X_9^{-1}) + Tr(\beta^{236}X_{14}^{-1}) + 0$$
$$f44 = Tr(\beta^{72}X_3^{-1}) + Tr(\beta^{72}X_4^{-1}) + Tr(\beta^{44}X_9^{-1}) + Tr(\beta^{237}X_{14}^{-1}) + 0$$
$$f45 = Tr(\beta^{76}X_3^{-1}) + Tr(\beta^{76}X_4^{-1}) + Tr(\beta^{72}X_9^{-1}) + Tr(\beta^{172}X_{14}^{-1}) + 1$$
$$f46 = Tr(\beta^{51}X_3^{-1}) + Tr(\beta^{51}X_4^{-1}) + Tr(\beta^{76}X_9^{-1}) + Tr(\beta^{52}X_{14}^{-1}) + 1$$
$$f47 = Tr(\beta^{26}X_3^{-1}) + Tr(\beta^{26}X_4^{-1}) + Tr(\beta^{51}X_9^{-1}) + Tr(\beta^{27}X_{14}^{-1}) + 0$$

$$f48 = Tr(\beta^{154}X_3^{-1}) + Tr(\beta^{166}X_4^{-1}) + Tr(\beta^{166}X_9^{-1}) + Tr(\beta^{26}X_{14}^{-1}) + 1$$
$$f49 = Tr(\beta^{100}X_3^{-1}) + Tr(\beta^{53}X_4^{-1}) + Tr(\beta^{53}X_9^{-1}) + Tr(\beta^{154}X_{14}^{-1}) + 1$$
$$f50 = Tr(\beta^{104}X_3^{-1}) + Tr(\beta^{36}X_4^{-1}) + Tr(\beta^{36}X_9^{-1}) + Tr(\beta^{53}X_{14}^{-1}) + 0$$
$$f51 = Tr(\beta^{236}X_3^{-1}) + Tr(\beta^{11}X_4^{-1}) + Tr(\beta^{11}X_9^{-1}) + Tr(\beta^{47}X_{14}^{-1}) + 0$$
$$f52 = Tr(\beta^{237}X_3^{-1}) + Tr(\beta^{72}X_4^{-1}) + Tr(\beta^{72}X_9^{-1}) + Tr(\beta^{44}X_{14}^{-1}) + 0$$
$$f53 = Tr(\beta^{172}X_3^{-1}) + Tr(\beta^{76}X_4^{-1}) + Tr(\beta^{76}X_9^{-1}) + Tr(\beta^{72}X_{14}^{-1}) + 1$$
$$f54 = Tr(\beta^{52}X_3^{-1}) + Tr(\beta^{51}X_4^{-1}) + Tr(\beta^{51}X_9^{-1}) + Tr(\beta^{76}X_{14}^{-1}) + 1$$
$$f55 = Tr(\beta^{27}X_3^{-1}) + Tr(\beta^{26}X_4^{-1}) + Tr(\beta^{26}X_9^{-1}) + Tr(\beta^{51}X_{14}^{-1}) + 0$$

$$f56 = Tr(\beta^{26}X_3^{-1}) + Tr(\beta^{154}X_4^{-1}) + Tr(\beta^{166}X_9^{-1}) + Tr(\beta^{166}X_{14}^{-1}) + 1$$
$$f57 = Tr(\beta^{154}X_3^{-1}) + Tr(\beta^{100}X_4^{-1}) + Tr(\beta^{53}X_9^{-1}) + Tr(\beta^{53}X_{14}^{-1}) + 1$$
$$f58 = Tr(\beta^{53}X_3^{-1}) + Tr(\beta^{104}X_4^{-1}) + Tr(\beta^{36}X_9^{-1}) + Tr(\beta^{36}X_{14}^{-1}) + 0$$
$$f59 = Tr(\beta^{47}X_3^{-1}) + Tr(\beta^{236}X_4^{-1}) + Tr(\beta^{11}X_9^{-1}) + Tr(\beta^{11}X_{14}^{-1}) + 0$$
$$f60 = Tr(\beta^{44}X_3^{-1}) + Tr(\beta^{237}X_4^{-1}) + Tr(\beta^{72}X_9^{-1}) + Tr(\beta^{72}X_{14}^{-1}) + 0$$
$$f61 = Tr(\beta^{72}X_3^{-1}) + Tr(\beta^{172}X_4^{-1}) + Tr(\beta^{76}X_9^{-1}) + Tr(\beta^{76}X_{14}^{-1}) + 1$$
$$f62 = Tr(\beta^{76}X_3^{-1}) + Tr(\beta^{52}X_4^{-1}) + Tr(\beta^{51}X_9^{-1}) + Tr(\beta^{51}X_{14}^{-1}) + 1$$
$$f63 = Tr(\beta^{51}X_3^{-1}) + Tr(\beta^{27}X_4^{-1}) + Tr(\beta^{26}X_9^{-1}) + Tr(\beta^{26}X_{14}^{-1}) + 0$$

$$
\begin{aligned}
f64 &= Tr(\beta^{166}X_2^{-1}) + Tr(\beta^{166}X_7^{-1}) + Tr(\beta^{26}X_8^{-1}) + Tr(\beta^{154}X_{13}^{-1}) + 1\\
f65 &= Tr(\beta^{53}X_2^{-1}) + Tr(\beta^{53}X_7^{-1}) + Tr(\beta^{154}X_8^{-1}) + Tr(\beta^{100}X_{13}^{-1}) + 1\\
f66 &= Tr(\beta^{36}X_2^{-1}) + Tr(\beta^{36}X_7^{-1}) + Tr(\beta^{53}X_8^{-1}) + Tr(\beta^{104}X_{13}^{-1}) + 0\\
f67 &= Tr(\beta^{11}X_2^{-1}) + Tr(\beta^{11}X_7^{-1}) + Tr(\beta^{47}X_8^{-1}) + Tr(\beta^{236}X_{13}^{-1}) + 0\\
f68 &= Tr(\beta^{72}X_2^{-1}) + Tr(\beta^{72}X_7^{-1}) + Tr(\beta^{44}X_8^{-1}) + Tr(\beta^{237}X_{13}^{-1}) + 0\\
f69 &= Tr(\beta^{76}X_2^{-1}) + Tr(\beta^{76}X_7^{-1}) + Tr(\beta^{72}X_8^{-1}) + Tr(\beta^{172}X_{13}^{-1}) + 1\\
f70 &= Tr(\beta^{51}X_2^{-1}) + Tr(\beta^{51}X_7^{-1}) + Tr(\beta^{76}X_8^{-1}) + Tr(\beta^{52}X_{13}^{-1}) + 1\\
f71 &= Tr(\beta^{26}X_2^{-1}) + Tr(\beta^{26}X_7^{-1}) + Tr(\beta^{51}X_8^{-1}) + Tr(\beta^{27}X_{13}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f72 &= Tr(\beta^{154}X_2^{-1}) + Tr(\beta^{166}X_7^{-1}) + Tr(\beta^{166}X_8^{-1}) + Tr(\beta^{26}X_{13}^{-1}) + 1\\
f73 &= Tr(\beta^{100}X_2^{-1}) + Tr(\beta^{53}X_7^{-1}) + Tr(\beta^{53}X_8^{-1}) + Tr(\beta^{154}X_{13}^{-1}) + 1\\
f74 &= Tr(\beta^{104}X_2^{-1}) + Tr(\beta^{36}X_7^{-1}) + Tr(\beta^{36}X_8^{-1}) + Tr(\beta^{53}X_{13}^{-1}) + 0\\
f75 &= Tr(\beta^{236}X_2^{-1}) + Tr(\beta^{11}X_7^{-1}) + Tr(\beta^{11}X_8^{-1}) + Tr(\beta^{47}X_{13}^{-1}) + 0\\
f76 &= Tr(\beta^{237}X_2^{-1}) + Tr(\beta^{72}X_7^{-1}) + Tr(\beta^{72}X_8^{-1}) + Tr(\beta^{44}X_{13}^{-1}) + 0\\
f77 &= Tr(\beta^{172}X_2^{-1}) + Tr(\beta^{76}X_7^{-1}) + Tr(\beta^{76}X_8^{-1}) + Tr(\beta^{72}X_{13}^{-1}) + 1\\
f78 &= Tr(\beta^{52}X_2^{-1}) + Tr(\beta^{51}X_7^{-1}) + Tr(\beta^{51}X_8^{-1}) + Tr(\beta^{76}X_{13}^{-1}) + 1\\
f79 &= Tr(\beta^{27}X_2^{-1}) + Tr(\beta^{26}X_7^{-1}) + Tr(\beta^{26}X_8^{-1}) + Tr(\beta^{51}X_{13}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f80 &= Tr(\beta^{26}X_2^{-1}) + Tr(\beta^{154}X_7^{-1}) + Tr(\beta^{166}X_8^{-1}) + Tr(\beta^{166}X_{13}^{-1}) + 1\\
f81 &= Tr(\beta^{154}X_2^{-1}) + Tr(\beta^{100}X_7^{-1}) + Tr(\beta^{53}X_8^{-1}) + Tr(\beta^{53}X_{13}^{-1}) + 1\\
f82 &= Tr(\beta^{53}X_2^{-1}) + Tr(\beta^{104}X_7^{-1}) + Tr(\beta^{36}X_8^{-1}) + Tr(\beta^{36}X_{13}^{-1}) + 0\\
f83 &= Tr(\beta^{47}X_2^{-1}) + Tr(\beta^{236}X_7^{-1}) + Tr(\beta^{11}X_8^{-1}) + Tr(\beta^{11}X_{13}^{-1}) + 0\\
f84 &= Tr(\beta^{44}X_2^{-1}) + Tr(\beta^{237}X_7^{-1}) + Tr(\beta^{72}X_8^{-1}) + Tr(\beta^{72}X_{13}^{-1}) + 0\\
f85 &= Tr(\beta^{72}X_2^{-1}) + Tr(\beta^{172}X_7^{-1}) + Tr(\beta^{76}X_8^{-1}) + Tr(\beta^{76}X_{13}^{-1}) + 1\\
f86 &= Tr(\beta^{76}X_2^{-1}) + Tr(\beta^{52}X_7^{-1}) + Tr(\beta^{51}X_8^{-1}) + Tr(\beta^{51}X_{13}^{-1}) + 1\\
f87 &= Tr(\beta^{51}X_2^{-1}) + Tr(\beta^{27}X_7^{-1}) + Tr(\beta^{26}X_8^{-1}) + Tr(\beta^{26}X_{13}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f88 &= Tr(\beta^{166}X_2^{-1}) + Tr(\beta^{26}X_7^{-1}) + Tr(\beta^{154}X_8^{-1}) + Tr(\beta^{166}X_{13}^{-1}) + 1\\
f89 &= Tr(\beta^{53}X_2^{-1}) + Tr(\beta^{154}X_7^{-1}) + Tr(\beta^{100}X_8^{-1}) + Tr(\beta^{53}X_{13}^{-1}) + 1\\
f90 &= Tr(\beta^{36}X_2^{-1}) + Tr(\beta^{53}X_7^{-1}) + Tr(\beta^{104}X_8^{-1}) + Tr(\beta^{36}X_{13}^{-1}) + 0\\
f91 &= Tr(\beta^{11}X_2^{-1}) + Tr(\beta^{47}X_7^{-1}) + Tr(\beta^{236}X_8^{-1}) + Tr(\beta^{11}X_{13}^{-1}) + 0\\
f92 &= Tr(\beta^{72}X_2^{-1}) + Tr(\beta^{44}X_7^{-1}) + Tr(\beta^{237}X_8^{-1}) + Tr(\beta^{72}X_{13}^{-1}) + 0\\
f93 &= Tr(\beta^{76}X_2^{-1}) + Tr(\beta^{72}X_7^{-1}) + Tr(\beta^{172}X_8^{-1}) + Tr(\beta^{76}X_{13}^{-1}) + 1\\
f94 &= Tr(\beta^{51}X_2^{-1}) + Tr(\beta^{76}X_7^{-1}) + Tr(\beta^{52}X_8^{-1}) + Tr(\beta^{51}X_{13}^{-1}) + 1\\
f95 &= Tr(\beta^{26}X_2^{-1}) + Tr(\beta^{51}X_7^{-1}) + Tr(\beta^{27}X_8^{-1}) + Tr(\beta^{26}X_{13}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f96 &= Tr(\beta^{154}X_1^{-1}) + Tr(\beta^{166}X_6^{-1}) + Tr(\beta^{166}X_{11}^{-1}) + Tr(\beta^{26}X_{12}^{-1}) + 1\\
f97 &= Tr(\beta^{100}X_1^{-1}) + Tr(\beta^{53}X_6^{-1}) + Tr(\beta^{53}X_{11}^{-1}) + Tr(\beta^{154}X_{12}^{-1}) + 1\\
f98 &= Tr(\beta^{104}X_1^{-1}) + Tr(\beta^{36}X_6^{-1}) + Tr(\beta^{36}X_{11}^{-1}) + Tr(\beta^{53}X_{12}^{-1}) + 0\\
f99 &= Tr(\beta^{236}X_1^{-1}) + Tr(\beta^{11}X_6^{-1}) + Tr(\beta^{11}X_{11}^{-1}) + Tr(\beta^{47}X_{12}^{-1}) + 0\\
f100 &= Tr(\beta^{237}X_1^{-1}) + Tr(\beta^{72}X_6^{-1}) + Tr(\beta^{72}X_{11}^{-1}) + Tr(\beta^{44}X_{12}^{-1}) + 0\\
f101 &= Tr(\beta^{172}X_1^{-1}) + Tr(\beta^{76}X_6^{-1}) + Tr(\beta^{76}X_{11}^{-1}) + Tr(\beta^{72}X_{12}^{-1}) + 1\\
f102 &= Tr(\beta^{52}X_1^{-1}) + Tr(\beta^{51}X_6^{-1}) + Tr(\beta^{51}X_{11}^{-1}) + Tr(\beta^{76}X_{12}^{-1}) + 1\\
f103 &= Tr(\beta^{27}X_1^{-1}) + Tr(\beta^{26}X_6^{-1}) + Tr(\beta^{26}X_{11}^{-1}) + Tr(\beta^{51}X_{12}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f104 &= Tr(\beta^{26}X_1^{-1}) + Tr(\beta^{154}X_6^{-1}) + Tr(\beta^{166}X_{11}^{-1}) + Tr(\beta^{166}X_{12}^{-1}) + 1\\
f105 &= Tr(\beta^{154}X_1^{-1}) + Tr(\beta^{100}X_6^{-1}) + Tr(\beta^{53}X_{11}^{-1}) + Tr(\beta^{53}X_{12}^{-1}) + 1\\
f106 &= Tr(\beta^{53}X_1^{-1}) + Tr(\beta^{104}X_6^{-1}) + Tr(\beta^{36}X_{11}^{-1}) + Tr(\beta^{36}X_{12}^{-1}) + 0\\
f107 &= Tr(\beta^{47}X_1^{-1}) + Tr(\beta^{236}X_6^{-1}) + Tr(\beta^{11}X_{11}^{-1}) + Tr(\beta^{11}X_{12}^{-1}) + 0\\
f108 &= Tr(\beta^{44}X_1^{-1}) + Tr(\beta^{237}X_6^{-1}) + Tr(\beta^{72}X_{11}^{-1}) + Tr(\beta^{72}X_{12}^{-1}) + 0\\
f109 &= Tr(\beta^{72}X_1^{-1}) + Tr(\beta^{172}X_6^{-1}) + Tr(\beta^{76}X_{11}^{-1}) + Tr(\beta^{76}X_{12}^{-1}) + 1\\
f110 &= Tr(\beta^{76}X_1^{-1}) + Tr(\beta^{52}X_6^{-1}) + Tr(\beta^{51}X_{11}^{-1}) + Tr(\beta^{51}X_{12}^{-1}) + 1\\
f111 &= Tr(\beta^{51}X_1^{-1}) + Tr(\beta^{27}X_6^{-1}) + Tr(\beta^{26}X_{11}^{-1}) + Tr(\beta^{26}X_{12}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f112 &= Tr(\beta^{166}X_1^{-1}) + Tr(\beta^{26}X_6^{-1}) + Tr(\beta^{154}X_{11}^{-1}) + Tr(\beta^{166}X_{12}^{-1}) + 1\\
f113 &= Tr(\beta^{53}X_1^{-1}) + Tr(\beta^{154}X_6^{-1}) + Tr(\beta^{100}X_{11}^{-1}) + Tr(\beta^{53}X_{12}^{-1}) + 1\\
f114 &= Tr(\beta^{36}X_1^{-1}) + Tr(\beta^{53}X_6^{-1}) + Tr(\beta^{104}X_{11}^{-1}) + Tr(\beta^{36}X_{12}^{-1}) + 0\\
f115 &= Tr(\beta^{11}X_1^{-1}) + Tr(\beta^{47}X_6^{-1}) + Tr(\beta^{236}X_{11}^{-1}) + Tr(\beta^{11}X_{12}^{-1}) + 0\\
f116 &= Tr(\beta^{72}X_1^{-1}) + Tr(\beta^{44}X_6^{-1}) + Tr(\beta^{237}X_{11}^{-1}) + Tr(\beta^{72}X_{12}^{-1}) + 0\\
f117 &= Tr(\beta^{76}X_1^{-1}) + Tr(\beta^{72}X_6^{-1}) + Tr(\beta^{172}X_{11}^{-1}) + Tr(\beta^{76}X_{12}^{-1}) + 1\\
f118 &= Tr(\beta^{51}X_1^{-1}) + Tr(\beta^{76}X_6^{-1}) + Tr(\beta^{52}X_{11}^{-1}) + Tr(\beta^{51}X_{12}^{-1}) + 1\\
f119 &= Tr(\beta^{26}X_1^{-1}) + Tr(\beta^{51}X_6^{-1}) + Tr(\beta^{27}X_{11}^{-1}) + Tr(\beta^{26}X_{12}^{-1}) + 0
\end{aligned}
$$

$$
\begin{aligned}
f120 &= Tr(\beta^{166}X_1^{-1}) + Tr(\beta^{166}X_6^{-1}) + Tr(\beta^{26}X_{11}^{-1}) + Tr(\beta^{154}X_{12}^{-1}) + 1\\
f121 &= Tr(\beta^{53}X_1^{-1}) + Tr(\beta^{53}X_6^{-1}) + Tr(\beta^{154}X_{11}^{-1}) + Tr(\beta^{100}X_{12}^{-1}) + 1\\
f122 &= Tr(\beta^{36}X_1^{-1}) + Tr(\beta^{36}X_6^{-1}) + Tr(\beta^{53}X_{11}^{-1}) + Tr(\beta^{104}X_{12}^{-1}) + 0\\
f123 &= Tr(\beta^{11}X_1^{-1}) + Tr(\beta^{11}X_6^{-1}) + Tr(\beta^{47}X_{11}^{-1}) + Tr(\beta^{236}X_{12}^{-1}) + 0\\
f124 &= Tr(\beta^{72}X_1^{-1}) + Tr(\beta^{72}X_6^{-1}) + Tr(\beta^{44}X_{11}^{-1}) + Tr(\beta^{237}X_{12}^{-1}) + 0\\
f125 &= Tr(\beta^{76}X_1^{-1}) + Tr(\beta^{76}X_6^{-1}) + Tr(\beta^{72}X_{11}^{-1}) + Tr(\beta^{172}X_{12}^{-1}) + 1\\
f126 &= Tr(\beta^{51}X_1^{-1}) + Tr(\beta^{51}X_6^{-1}) + Tr(\beta^{76}X_{11}^{-1}) + Tr(\beta^{52}X_{12}^{-1}) + 1\\
f127 &= Tr(\beta^{26}X_1^{-1}) + Tr(\beta^{26}X_6^{-1}) + Tr(\beta^{51}X_{11}^{-1}) + Tr(\beta^{27}X_{12}^{-1}) + 0
\end{aligned}
$$

8 Appendix II The matrix Transformation for Example 3

$$A_{31,0} = \begin{bmatrix}
I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & A_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_{10} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & A_{15}
\end{bmatrix},$$

where I denotes an 8×8 identity matrix, 0 denotes zero matrices of the same dimension. A_5, A_{10} and A_{15} are given by

$$A_5 = \begin{bmatrix}
0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 0
\end{bmatrix}, A_{10} = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 1
\end{bmatrix}, A_{15} = \begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0
\end{bmatrix}.$$