# On Steiner Triple Systems and Perfect Codes

Mats Näslund
ERA/T/NG
Ericsson Radio
SE - 164 80
Stockholm, Sweden

**Abstract**

Using a computer implementation, we show that two more of the Steiner triple systems on 15 elements are perfect, i.e. that there are binary perfect codes of length 15, generating STS which have rank 15. This answers partially a question posed by Hergert in [3].

We also briefly study the inverse problem of generating a perfect code from a Steiner triple system using a greedy algorithm. We obtain codes that were not previously known to be generated by such procedures.

**Keywords:** Steiner triple system, perfect code

# 1 Introduction

In this paper we will study the relation between binary perfect one-error correcting codes of length 15 and Steiner triple systems (STS) on 15 elements. Thus, we will simply by *perfect code* and *STS* refer to the above.

It is well known that every perfect code generates at least one STS by considering the codewords of Hamming weight 3 as blocks of a STS. For length 15 codes, Phelps showed in [6] that the converse was true for all STS of rank at most 14, i.e. all such STS are *perfect*. However, not a single one of the STS with full rank was known to be generated by a perfect code. This is not too surprising since it is easy to see that if $S$ is generated by $C$, then $\text{rank}(S) \leq \text{rank}(C) = 15 - \text{codim}(C)$ and all previously known perfect codes had $\text{codim}(C) \geq 1$. The constructions by Heden in [2] are the first examples of perfect codes with codimension equal to zero, and are therefore also the first candidates to generate a STS of maximum rank. Using these new codes we show that at least two different (non-isomorphic) STS of rank 15 are perfect. We thus increase the number of known perfect STS from 23 to 25.

The procedure of generating a STS from a perfect code is straight-forward but one can ask if it is possible reverse the procedure: start with a STS and expand

| *Code* | rank($C$) | *Generated STS (cf. [4])* |
|---|---|---|
| $C_{11}, C_{22}$ | 14 | 1,2,3,4,5,8,9,10,12 |
| $C_{12}$ | 15 | 1,2,4,9,12,24,29 |
| $C_{14}, C_{25}$ | 14 | 1,2,3,4,5,8,9,10,12 |
| $C_{15}, C_{16}, C_{24}, C_{26}$ | 15 | 1,2,4,9,12,24,29 |
| $C_{32}, C_{13}$ | 14 | 1,2,4,9,12 |
| $C_{33}$ | 13 | 1,2,4 |
| $C_{34}, C_{35}, C_{36}$ | 14 | 1,2,4,9,12 |
| $C_{44}, C_{55}, C_{66}$ | 14 | 2,3,4,5,8,9,10 |
| $C_{45}, C_{46}, C_{56}$ | 15 | 2,4,9,12,24,29 |
| $C_3$ | 14 | 1,2,3,4,5,8,9,10 |

Table 1: Generated STS from the new codes

this to a perfect code. Conway and Sloane, [1], gave a simple greedy algorithm that will generate the well known Hamming code by selecting, in lexicographic order, codewords in $\mathbb{Z}_2^{15}$ at distance at least 3 from the ones previously selected. We found that a similar procedure works starting from several different STS and will give codes other than the Hamming code. We have no explanation for why this works, but some further studies might give some interesting results.

This paper is an extract from [5], to which we refer for further details.

## 2 Steiner triple systems from perfect codes

The codes in [2] can be expressed as $C_{ij} = C(A_i, A_j)$, where the $A_i$s are MDS-codes over GF$(4)^4$. It turns out that there are six different $A_i$s that can be used, giving us a total of 21 such codes to study ($C_{ij}$ gives the same STS as $C_{ji}$). Finally, we have the code $C_3$ from [2] that has a slightly different construction.

Since the codes are non-linear, we make sure the codes we study contain the word $00\cdots0$ by forming all possible cosets: $\{x+y \mid y \in C_{ij}\}$ for all $x \in C_{ij}$. Furthermore, the codes $C_{ij}$ are extended codes of length 16 so there are 16 ways of deleting a coordinate from the code (puncturing) to get a length 15 code, so we try them all too. Hence, each $C_{ij}$ gives $2^{11} \cdot 16$ codes of length 15 (of which many may be equivalent). To identify the different STS generated by each of these codes, we compute the STS's rank and its so called *compact train*. These two parameters distinguish uniquely between all 80 non-isomorphic STS on 15 elements as listed in [4].

Table 1 summarizes the results. The identity numbers of the STS are those in [4]. Systems no. 24 and 29 have rank 15 and are hence the first example of such generated by a perfect code.

| Used STS | Generated code | | |
| --- | --- | --- | --- |
| *STS no (cf. [4])* | rank($C$) | dim(ker($C$)) | *Generated STS* |
| 1 | 11 | 11 | 1 |
| 2 | 12 | 8 | 1,2 |
| 3* | 13 | 5 | 1,2,3,4,5 |
| 4* | 13 | 4 | 1,2,4 |
| 12* | 14 | 2 | 1,2,4,9,12 |

Table 2: Generated codes from STS

# 3 Perfect codes from Steiner triple systems

Starting with a STS we interpreted the blocks as the codewords of weight 3 in a perfect code and tried different schemes of adding more words to actually obtain a perfect code. In particular, we tried the following method.

Order all candidate codewords in $\mathbb{Z}_2^{15}$ by increasing Hamming weight. Settle ties by defining $x < y$ if $x$ precedes $y$ in the normal lexicographic order. Try words of weights 4,5,6 and 7 in the above order and add every word at distance at least 3 from all the ones already chosen. Finally, for each codeword also add its complement (giving words of weight $\geq 8$). It then suffices to check that the distances between words of weights 7, 8 and 9 are also at least 3. When this greedy algorithm succeeded, giving a perfect code $C$, we ran the "backwards" method described in the previous section to see which STS were generated by $C$. The results are found in Table 2.

All 80 STS in [4] have been tried and as can be seen we succeeded in five cases. The STS marked '*' are systems isomorphic to those in [4] and can be found in the Appendix.

A few notes: We tried other greedy strategies, but none has been successful. For instance, we tried applying randomly chosen permutations to the STS before starting the greedy algorithm but this does not seem to help.

**Acknowledgment.** I would like to take the opportunity to thank Olof Heden for suggestions and encouragement.

# References

[1] J.H. Conway and N.J.A. Sloane, *Lexicographic Codes: Error-Correcting Codes from Game Theory.* IEEE Transactions on Information Theory, **IT-32** (1986), no 3, 337–348.

[2] O. Heden, *A Binary Perfect Code of Length 15 and Codimension 0.* Designs, Codes and Cryptography, **4** (1994), 213–220..

[3] F. Hergert, *Algebraische Methoden für nichtlineare Codes.* Thesis, Darmstadt, 1984.

[4] R.A. Mathon, K.T. Phelps and A. Rosa, *Small Steiner Triple Systems and Their Properties.* Ars Combinatoria, **15** (1983), 3–110.

[5] M. Näslund, *Steiner Triple Systems and Perfect Codes.* MSc thesis TRITA-MAT-1993-0007, Dept of Mathematics, KTH, Stockholm, 1993.

[6] K.T. Phelps, *A Combinatorial Construction of Perfect Codes.* Siam J. Alg. and Discrete Methods, 4 (1983), 398–403.

# A Steiner triple systems used to generate perfect codes

The following three STS were used to generate perfect codes. They are isomorphic to systems 3, 4 and 12 (listed in this order) in [4].

| | | | | | |
|---|---|---|---|---|---|
| {1,2,3} | {1,4,5} | {1,6,7} | {1,8,11} | {1,9,10} | {1,12,13} |
| {1,14,15} | {2,4,6} | {2,5,7} | {2,8,10} | {2,9,11} | {2,12,14} |
| {2,13,15} | {3,4,15} | {3,5,14} | {3,6,13} | {3,7,12} | {3,8,9} |
| {3,10,11} | {4,7,11} | {4,8,2} | {4,9,13} | {4,10,14} | {5,6,11} |
| {5,8,13} | {5,9,12} | {5,10,15} | {6,8,14} | {6,9,15} | {6,10,12} |
| {7,8,15} | {7,9,14} | {7,10,13} | {11,12,15} | {11,13,14} | |

| | | | | | |
|---|---|---|---|---|---|
| {1,2,3} | {1,4,7} | {1,5,6} | {1,8,9} | {1,10,11} | {1,12,13} |
| {1,14,15} | {2,4,6} | {2,5,7} | {2,8,10} | {2,9,11} | {2,12,14} |
| {2,13,15} | {3,4,5} | {3,6,7} | {3,8,15} | {3,9,10} | {3,11,12} |
| {3,13,14} | {4,8,12} | {4,9,13} | {4,10,14} | {4,11,15} | {5,8,13} |
| {5,9,12} | {5,10,15} | {5,11,14} | {6,8,14} | {6,9,15} | {6,10,12} |
| {6,11,13} | {7,8,11} | {7,9,14} | {7,10,13} | {7,12,15} | |

| | | | | | |
|---|---|---|---|---|---|
| {1,2,3} | {1,4,7} | {1,5,6} | {1,8,9} | {1,10,11} | {1,12,13} |
| {1,14,15} | {2,4,6} | {2,5,15} | {2,7,13} | {2,8,10} | {2,9,11} |
| {2,12,14} | {3,4,5} | {3,6,7} | {3,8,15} | {3,9,10} | {3,11,12} |
| {3,13,14} | {4,8,12} | {4,9,13} | {4,10,14} | {4,11,15} | {5,7,10} |
| {5,8,13} | {5,9,12} | {5,11,14} | {6,8,14} | {6,9,15} | {6,10,12} |
| {6,11,13} | {7,8,11} | {7,9,14} | {7,12,15} | {10,13,15} | |