Irregular Product Codes

Masoud Alipour*, Omid Etesami*, Ghid Maatouk*, Amin Shokrollahi*
*Laboratoire d'algorithmique, École Polytechnique Fédérale de Lausanne
{firstname.lastname}@epfl.ch

***Abstract*—We consider irregular product codes. In this class of codes, each codeword is represented by a matrix. The entries in each row (column) of the matrix should come from a component row (column) code. As opposed to (standard) product codes, we do not require that all component row codes nor all component column codes be the same. As we will see, relaxing this requirement can provide some additional attractive features including 1) allowing some regions of the codeword be more error-resilient 2) allowing a more refined spectrum of rates for finite-lengths and improved performance in some of these rates 3) more interaction between row and column codes during decoding.**

We study these codes over erasure channels. We find that for any $0 < \epsilon < 1$, for many rate distributions on component row codes, there is a matching rate distribution on component column codes such that an irregular product code based on MDS codes with those rate distributions on the component codes has asymptotic rate $1 - \epsilon$ and can decode on erasure channels (of alphabet size equal the alphabet size of the component MDS codes) with erasure probability $< \epsilon$.

I. Introduction

Product codes were introduced in 1954 by Elias [1]. A product code can be viewed as a special case of Tanner construction [2] in which smaller constituent codes make a larger code with low complexity decoding. An $m \times n$ product code is defined by a *row code* C of length n and rate r_C, and a *column code* C' of length m and rate $r_{C'}$. Codewords are represented by $m \times n$ matrices which satisfy the constraint that every row belongs to C and every column to C'. Product codes are decoded in an iterative fashion, where rows and columns are recovered in successive rounds using the decoders for C and C'. The rate of the product code is the product of the rates r_C and $r_{C'}$.

In this work, we present irregular product codes, a generalization of product codes in which we do not require that the rows (columns) belong to a single code. We will show that while these codes still retain the advantages of product codes, they present some additional attractive features.

One of the main advantages of product codes is the fact that decoding takes place over the smaller component codes, which can result in a speedup of decoding. Furthermore, by combining Reed-Solomon component codes, one can obtain product codes which have length equal to the square of the size of the component codes for the same field size, while taking advantage of the MDS properties of the small component codes.

Another (more application-specific) feature of product codes is that they perform well on bursty channels. Indeed, for a product code which is transmitted row by row, a burst error will corrupt several consecutive rows but spread evenly over columns, thus allowing the column codes to recover the corrupted entries.

Irregular product codes are based on the simple idea that we need not restrict ourselves to a single row and column code, but instead allow row and column codes of multiple rates. The intuition behind this is that allowing for a few low-rate, highly error-resilient codes might boost the decoding process, while other high-rate codes ensure that the overall irregular product code has good rate. With a careful design of the rate distributions, one can hope to achieve better performance than for regular product codes. Irregularity has been a powerful concept in many contexts; e.g., irregular degree distributions for LDPC codes, LT codes, etc. This idea fully exploits the inherently interactive nature of the decoding of product codes. Indeed, round-based decoding of product codes lets some rows and columns "help" others to recover and go on with the decoding process. Allowing for various decoding capabilities for different rows and columns only taps further into this property of the decoder. [1]

Irregular product codes retain the advantages of product codes, while presenting additional features that make them more attractive. Decoding still takes place over smaller codes and the field size is still allowed to grow slower in the case of MDS component codes. Further, not only do irregular product codes still perform well on bursty channels, they can also be more powerful than regular product codes when some parts of the codeword are

[1] Indeed, in product codes that achieve rates close to Shannon limit (say on erasure channels), either the row/column code (say row code) should have rate close to 1. In this case, the decoding happens first in the column codes whose rate is far from 1, and then the row codes play a "complementary" role. As we will see, there exist irregular product codes with rate vs. decoding capacity matching these product codes in which the row codes and column codes have the same distribution of rates, and the decoding process involves a longer and gradual interaction between row and column component codes.

known to be more vulnerable to bursts than others, since the row and column codes error-correction capabilities are tunable.

Moreover, for short-length linear codes, there do not exist product codes of every desirable dimension, since fixing the dimension of the product code leaves few choices for the dimensions of the component codes. Irregular product codes, on the other hand, allow for many more dimensions due to the numerous choices for the rate distribution of the component codes.

In this work, we first derive bounds on the rate and minimum distance of irregular product codes, and give constructions that achieve these bounds. We then give explicit families of irregular product codes that can get rates arbitrarily close to $1-\epsilon$ on channels with erasure ϵ based on MDS component codes. Note however that this does not mean that these codes are capacity-approaching in the sense of Shannon capacity because the field size for MDS codes can grow as a function of the length.[2]

We give simulation results for finite-length codes that show that irregular product codes have better thresholds than product codes of the same dimension or close dimension for some specific lengths.

Related works: Since the introduction of the product codes [1] many extensions have been proposed and these codes have found many applications from magnetic recording [3] to deep space communication [4] mainly because of their simple construction and low complexity decoding.

The use of different component codes for rows and different component codes for columns is not new. In fact, [5] and [6] consider product codes for image transmission where the rows are LDPC codes and the columns are RS codes with different rates. They determine the optimum rate of the RS codes by a dynamic programming.

However, to the best of our knowledge, irregular product codes with the generality considered in this paper together with some of their asymptotic behavior have not been previously similarly explored.

Multidimensional product codes are investigated in [7] and [8]. However, the component codes are restricted to be single parity and extended Hamming codes. In these papers, the authors devise a low complexity soft decoding algorithm for AWGN channels.

The weight distribution of some instances of product codes is known. For example, [9] analyzes the error floor region of an extended Hamming product code by means of the weight enumerator of the code and the union bound. Some characterization of the stopping sets over the erasure channel is obtained in [10] based on the minimum distance of the component codes. [11] tries to optimize the design of a product code where the component codes are limited to single parity codes and certain extended Hamming and BCH codes.

Product codes can be decoded iteratively using a message passing algorithm in noisy channels. Because of this, they are also referred to as turbo block codes [12] in the literature of coding theory.

The Tanner graph of the product code is regular. [13] considers product codes as structured generalized LDPC codes.

For a thorough survey on product codes refer to [14].

Organization of the Paper: The remainder of the paper is organized as follows. In Section II, we define irregular product codes. In Section III, we derive an upper bound on their dimension, and prove that under certain conditions, this upper bound can be achieved. In Section IV, we also derive a lower bound on the minimum distance of irregular product codes and show that sometimes this lower bound is achieved. In Section V, we turn to the asymptotic analysis of irregular product codes on erasure channels under the iterative decoding which switches back and forth between rows and columns. In Section VI, we give explicit families of irregular product codes based on MDS component codes that achieve rates close to what capacity-achieving codes achieve. Finally, in Section VII, we give some irregular product code constructions for specific code lengths and show by simulation that these constructions outperform regular product code of the same (or approximately the same) dimension.

We omit all the proofs in the conference version of the paper for the sake of space. Full proofs can be found in the full version of the paper.

II. Definition

We denote the set $\{1,\dots,m\}$ by $[m]$.

Definition 1. *Let $\mathbb{F}$ be a field and let m,n be positive integers. For each $i\in[m]$ let C_i be a code of length n over $\mathbb{F}$ and for each $j\in[n]$ let C'_j be a code of length m over $\mathbb{F}$.*

The $m\times n$ irregular product code $\mathcal{C}=\mathcal{C}(\{C_i\}_i,\{C'_j\}_j)$ is the code of length mn over $\mathbb{F}$ such that

$$\mathcal{C}=\{(c_{ij})_{i\in[m],j\in[n]}| \\ \forall i\ (c_{i1},\dots,c_{in})\in C_i;\forall j,(c_{1j},\dots,c_{mj})\in C'_j\}.$$

In the above definition, when all the codes C_i corresponding to the rows are equal and all the codes C'_j corresponding to the columns are equal, we obtain a standard product code.

[2] On the other hand, one can show that our analysis can be extended to the situation where instead of MDS codes as component codes, we use capacity-approaching codes of the same rate but over a fixed erasure channel, say BEC. In this case, the resulting product code will be truly capacity-approaching.

III. Rate of Irregular Product Codes

Theorem 2. *Consider an $m \times n$ irregular product code $\mathcal{C} = \mathcal{C}(\{C_i\}_i, \{C'_j\}_j)$. Let $0 \leq a_1 \leq \ldots \leq a_m \leq n$ and $0 \leq b_1 \leq \ldots \leq b_n \leq m$ be two integer sequences. For $i \in [m]$, assume that the value of the first a_i coordinates of any codeword in C_i can generate the remaining coordinates (in the sense that the values of these remaining coordinates are a function of the values of the first a_i coordinates). Similarly, for each $j \in [n]$, assume that the first b_j coordinates of any codeword in C'_j can generate the remaining coordinates. Then*

1) *$\mathcal{C}$ has dimension at most*

$$k_{\mathcal{C}} := \sum_{j=1}^{n} \sum_{i=b_{j-1}+1}^{b_j} \max(a_i - j + 1, 0), \quad (1)$$

where we define $b_0 := 0$.

2) *If furthermore for all $i \in [m], j \in [n]$, C_i is a linear code of dimension a_i and C'_j is a linear code of dimension b_j, and $C_1 \subseteq \cdots \subseteq C_m$ and $C'_1 \subseteq \cdots \subseteq C'_n$, then $\mathcal{C}$ has dimension exactly $k_{\mathcal{C}}$ as given by (1).*

IV. Minimum Distance of Irregular Product Codes

The following theorem gives the best general lower bound on the minimum distance of an irregular product code in terms of the minimum distances of the individual row and column codes. Notice that this does not preclude the possibility of obtaining better lower bounds if we know more about the row and column codes.

Theorem 3. *For two integer sequences $n \geq d_1 \geq \ldots \geq d_m \geq 1$ and $m \geq d'_1 \geq \ldots \geq d'_n \geq 1$, define*

$$D = \min_{1 \leq i \leq m-d_j+1; 1 \leq j \leq n-d_i+1} \max_{i-1 \leq i' \leq m; j-1 \leq j' \leq n} - (i'-i+1)(j'-j+1) + \sum_{k=i}^{i'} d_k + \sum_{k=j}^{j'} d'_k.$$

The number D is the minimum weight of a binary nonzero $m \times n$ matrix where every nonzero row i has weight $\geq d_i$ and every nonzero column j has weight $\geq d'_j$. Therefore, if $\mathcal{C} = \mathcal{C}(\{C_i\}_i, \{C'_j\}_j)$ is an $m \times n$ product code such that mindist$(C_i) = d_i$ and mindist$(C'_j) = d'_j$, then mindist$(\mathcal{C}) \geq D$. On the other hand, for any two sequences $n \geq d_1 \geq \ldots \geq d_m \geq 1$ and $m \geq d'_1 \geq \ldots \geq d'_n \geq 1$, there exist row codes C_i and column codes C'_j with mindist$(C_i) = d_i$ and mindist$(C'_j) = d'_j$, such that mindist$(\mathcal{C}) = D$.

V. Asymptotic Analysis of Decoding Irregular Product Codes on Erasure Channels

We need the following definition for the next theorem.

Definition 4. *Consider an $m \times n$ irregular product code $\mathcal{C} = \mathcal{C}(\{C_i\}_i, \{C'_j\}_j)$. We are interested in the asymptotic behavior of $\mathcal{C}$, therefore we think of $\mathcal{C}$ not individually but as one member of a family of irregular product codes where m and n grow. Suppose that $\alpha, \beta : [0,1] \to [0,1]$ are non-decreasing real functions. We say that the row and column codes have asymptotic normalized minimum distance distribution α and β if for every $\delta_1, \delta_2 > 0$, for large enough m and n, for each $i \in [m], j \in [n]$ we have $|$mindist$(C_i)/n - \alpha(x)| \leq \delta_1$ for some x such that $|1 - i/m - x| \leq \delta_2$ and $|$mindist$(C'_j)/m - \beta(y)| \leq \delta_1$ for some y such that $|1 - j/n - y| \leq \delta_2$.*

Theorem 5. *Assume an $m \times n$ product code $\mathcal{C} = \mathcal{C}(\{C_i\}_i, \{C'_j\}_j)$ having asymptotic normalized minimum distance distribution α and β as in Definition 4. Assume that neither of m or n grows exponentially or faster in terms of the other one. Consider that a codeword in $\mathcal{C}$ is sent over an erasure channel where each symbol is erased with probability $\epsilon > 0$. We iteratively decode row codes and column codes of $\mathcal{C}$ whenever the number of erasures in a row or column is smaller than the minimum distance of the code corresponding to that row or column. Assume that*

$$\alpha^{-1}(\epsilon \beta^{-1}(\epsilon x)) < x \text{ for all } x \in (0,1], \quad (2)$$

where we define $\beta^{-1}(x) = \sup(S_x)$ for $S_x = \{z \in [0,1] : \beta(z) \leq x\}$ if $S_x \neq \emptyset$ and we define $\beta^{-1}(x) = 0$ if $S_x = \emptyset$. We define α^{-1} similarly. Then for any constant $\delta_0 > 0$, for large enough codes in the family, all except a δ_0-fraction of the symbols can be decoded except with a probability exponentially small in $\min(m, n)$.

VI. Irregular Product Codes from MDS Codes

Proposition 6. *Consider an irregular product code $\mathcal{C} = \mathcal{C}(\{C_i\}_i, \{C'_j\}_j)$ where C_i is an $[n, a_i]$-MDS code and C'_j is an $[m, b_j]$-MDS code for all i, j. If $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$ are non-decreasing sequences, then the dimension of C is upper-bounded by formula (1).*

Furthermore, given any two integer sequences $0 \leq a_1 \leq \ldots \leq a_m \leq n$ and $0 \leq b_1 \leq \ldots \leq b_n \leq m$, we can meet this upper-bound in the following way. Choose n distinct elements $\alpha_1, \ldots, \alpha_n$ and m distinct elements $\beta_1, \ldots, \beta_m$ of the symbol field $\mathbb{F}$. Let V be the $a_m \times n$ Vandermonde matrix $V_{ij} = \alpha_j^{i-1}$ and V' be the $b_n \times m$ Vandermonde matrix $V'_{ij} = {\beta_j}^{i-1}$. Let C_i be the Reed-Solomon code having as generator matrix the first a_i rows of the matrix V and C'_j be the Reed-Solomon code having

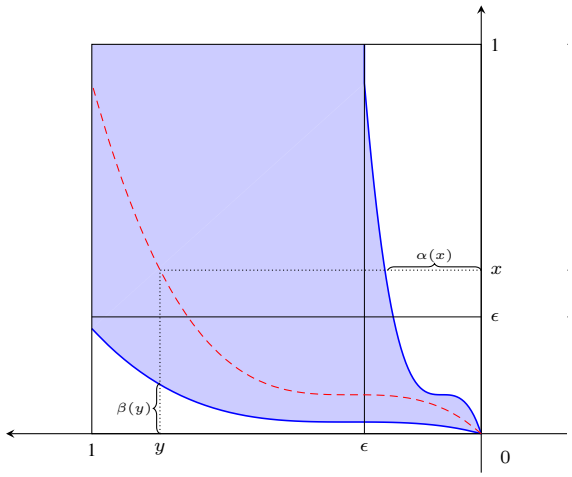

Fig. 1. This figure shows how the curve for α is obtained from the curve for β in Theorem 7. We stretch the curve for β vertically by a factor of $1/\epsilon$, and then shrink the curve for α horizontally by a factor of ϵ. That is, whenever $x = \beta(y)/\epsilon$, we have $\alpha(x) = \epsilon y$. The area of the shaded region denotes the asymptotic rate of the code, which is $1 - \epsilon$.

as generator matrix the first b_j rows of V'. Then the dimension of C is given exactly by formula (1).

Theorem 7. *For each $\epsilon > 0$, the following is a generic way of constructing families of irregular product codes with asymptotic rate $1-\epsilon$ such that for any constant $\delta > 0$ one can decode almost all the symbols of a codeword sent over an erasure channel having erasure probability $\epsilon - \delta$:*

Choose any non-decreasing function $\beta : [0,1] \to [0,1]$ with $\beta(1) \leq \epsilon$ and $\lim_{y\to 0} \beta(y) = 0$. Define $\alpha : [0,1] \to [0,1]$ by $\alpha(x) = \epsilon\beta^{-1}(\epsilon x)$ where β^{-1} is defined in Theorem 5. Choose m and n as you wish but neither of m or n should grow exponentially or faster in the other one. Then choose $0 \leq a_1 \leq \ldots \leq a_m \leq n$ and $0 \leq b_1 \leq \ldots \leq b_n \leq m$ as you wish but in such a way that $a_i = n(1 - \alpha(1 - i/m + o(1)) + o(1))$ and $b_j = m(1 - \beta(1 - j/n + o(1)) + o(1))$. Then choose the row codes C_i to be nested linear MDS codes of dimension a_i (for example as in Proposition 6). Choose similarly column codes C'_j of dimension b_j.

We note that the only regular products codes based on MDS codes which have decoding properties asymptotically as good as those constructed in Theorem 7 are codes where either $\alpha = 0$ or $\beta = 0$. These are regular product codes in which the row codes or column codes have rate $1 - o(1)$.

VII. Examples of Finite-Length Irregular Product Codes

In order to find an example of an irregular product code for finite but not so small lengths, say 50×50, we used the asymptotic irregular product code shown in Figure 2 obtained from Theorem 7, in which $\alpha(x) = \epsilon x$ and $\beta(y) = \epsilon y$ where ϵ is the erasure probability. The area of the shaded region, which represents the systematic part of the code, is the rate $1 - \epsilon$ of the code.

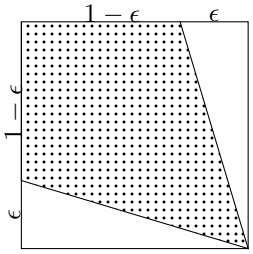

Fig. 2. The shaded region corresponds to the systematic or information part of the code by choosing $\alpha(x) = \epsilon x$ and $\beta(y) = \epsilon y$ where ϵ is the erasure probability.

Next we slightly tuned the asymptotic code to a 50×50 irregular product code in such a way that

- the code can start decoding better, by increasing the number of row and column codes having the highest minimum distance by a few;
- more importantly, the code has a much higher probability of decoding all symbols once most of the symbols have been decoded, by forcing that the minimum distances of all row and column codes are at least some positive number, in this case 3.

We chose all row codes and all column codes to be nested MDS codes according to Theorem 6. The resulting code has a systematic part which is shown in Figure 3.

This code is a $[2500, 1709]$ code of rate 0.6836. We compared this code to all regular product codes having rates $[0.6708, 0.684]$. Note that most of these codes have rate even lower than this code. The result of the simulation is shown in Figure 4. This plot shows the block/word error rate of the code in an erasure channel with erase probability ϵ. All constituent row and column codes in irregular and regular cases are considered to be MDS with the corresponding dimensions. Each point of

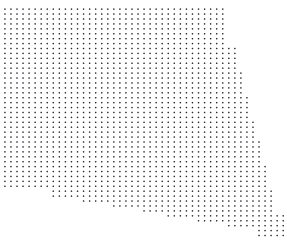

Fig. 3. Systematic part of a $[2500, 1709]$ irregular product code

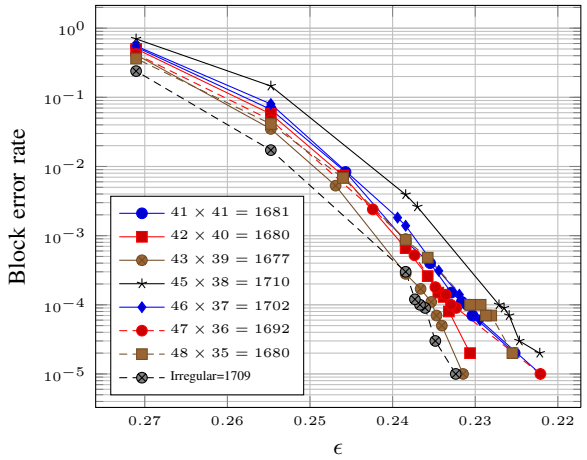

Fig. 4. Comparing an irregular $[2500, 1709]$ code to almost equal rate regular ones. The number on the legends indicate the corresponding row and column dimensions.

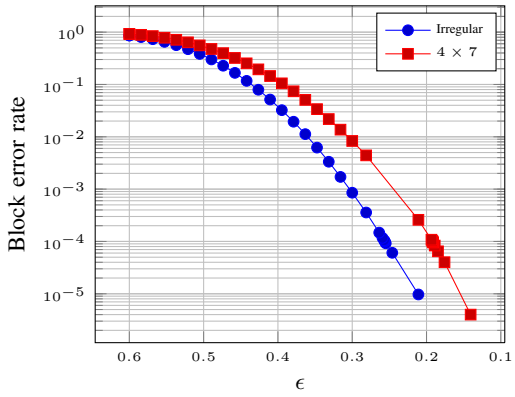

Fig. 5. Comparing an 8×8 regular and irregular product codes both with dimension 28

these curves is obtained by 10^6 simulations. The erasure patterns for different values of ϵ have been coupled such that the block error versus erasure probability curve is monotonic. One can see that this code outperforms all product codes having lower rates.

Figures 5 and 6 show another case where an irregular code outperforms a regular code for a much smaller length. We compared a regular $[8 \times 8, 4 \times 7]$ product code with an irregular code which is shown in Figure 6. Numbers on rows and columns indicate the dimension of the corresponding row and column MDS code. The block error probability of these codes is shown in Figure 5. Both codes are $[64, 28]$ codes.

ACKNOWLEDGEMENT

This work was supported by Grant 228021-ECCSciEng of the European Research Council.

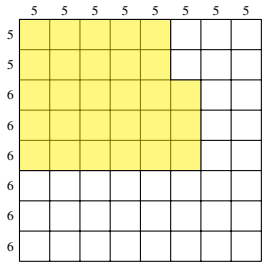

Fig. 6. Systematic part of an $[8 \times 8, 28]$ irregular product code is shaded

REFERENCES

[1] P. Elias, "Error-free coding," *IEEE Transactions on Information Theory*, vol. 4, no. 4, pp. 29–37, Sep. 1954.

[2] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[3] P. Chaichanavong and P. Siegel, "Tensor-product parity code for magnetic recording," *IEEE Transactions on Magnetics*, vol. 42, no. 2, pp. 350–352, Feb. 2006.

[4] M. Baldi, G. Cancellieri, and F. Chiaraluce, "A class of Low-Density Parity-Check product codes," in *Advances in Satellite and Space Communications, 2009. SPACOMM 2009. First International Conference on*, Jul. 2009, pp. 107 –112.

[5] V. Stankovic, R. Hamzaoui, and Z. Xiong, "Joint product code optimization for scalable multimedia transmission over wireless channels," in *Multimedia and Expo, 2002. ICME '02. Proceedings. 2002 IEEE International Conference on*, vol. 1, 2002, pp. 865 – 868 vol.1.

[6] L. Cao and C. W. Chen, "A novel product coding and recurrent alternate decoding scheme for image transmission over noisy channels," *Communications, IEEE Transactions on*, vol. 51, no. 9, pp. 1426 – 1431, Sep. 2003.

[7] D. Rankin and T. Gulliver, "Single parity check product codes," *Communications, IEEE Transactions on*, vol. 49, no. 8, pp. 1354 –1362, Aug. 2001.

[8] D. Rankin, T. Gulliver, and D. Taylor, "Asymptotic performance of single parity-check product codes," *Information Theory, IEEE Transactions on*, vol. 49, no. 9, pp. 2230 – 2235, Sep. 2003.

[9] F. Chiaraluce and R. Garello, "Extended hamming product codes analytical performance evaluation for low error rate applications," *IEEE Transactions on Wireless Communications*, vol. 3, no. 6, pp. 2353–2361, Nov. 2004.

[10] E. Rosnes, "Stopping set analysis of iterative Row-Column decoding of product codes," *IEEE Transactions on Information Theory*, vol. 54, no. 4, pp. 1551–1560, Apr. 2008.

[11] Y. Blankenship, B. Classon, and V. Desai, "Block product code design with the aid of union bounds," in *Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st*, vol. 3, Jun. 2005, pp. 1533 – 1537 Vol. 3.

[12] R. Pyndiah, "Near-optimum decoding of product codes: block turbo codes," *IEEE Transactions on Communications*, vol. 46, no. 8, pp. 1003–1010, Aug. 1998.

[13] M. Lentmaier, G. Liva, E. Paolini, and G. Fettweis, "From product codes to structured generalized LDPC codes," in *Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on*, Aug. 2010, pp. 1 –8.

[14] F. R. Kschischang, "Product codes," in *Wiley Encyclopedia of Telecommunications*. Hoboken, NJ, USA: John Wiley & Sons, Inc., Apr. 2003.