Upper bounds on separating codes

Gérard D. Cohen, *Senior Member, IEEE*
Hans Georg Schaathun, *Member, IEEE*

***Abstract*— The combinatorial concept of separating systems has numerous applications, such as automata theory, digital fingerprinting, group testing, and hashing. In this paper, we derive upper bounds on the size of codes with various separating properties.**

***Index Terms*— separating systems, superimposed codes, hashing, error-correcting codes**

An $(n, M, d)_q$ code is a set of M words of length n over an alphabet of q elements, at minimum distance d apart. If the code forms a linear vector space of dimension $k = \log_q M$ over $\mathsf{GF}(q)$, then we call it an $[n, k, d]_q$ code. A (t, u)-separating code, also known as a (t, u)-separating system or (t, u)-SS, is defined as follows.

Definition 1: A pair (T, U) of disjoint sets of words is called a (t, u)-configuration if $\#T = t$ and $\#U = u$. Such a configuration is separated if there is a position i, such that every word of T is different from any word of U on position i.

A code is (t, u)-separating if every (t, u)-configuration is separated.

The separating weight $\theta(T, U)$ of a (t, u)-configuration is the number of positions i which separate it. The (t, u)-separating weight $\theta_{t,u}$ of a code C is the minimum of $\theta(T, U)$ for all (t, u)-configurations (T, U). Note that $\theta_{1,1} = d$. In this paper we present improvements on the upper bounds on (t, u)-separating codes.

I. Motivation

The theory of separating systems has been applied in different areas of science and technology such as automata synthesis, technical diagnosis, constructions of hash functions, and authenticating ownership claims. Separating codes is a combinatorial concept and has been studied as such in a set-theoretic framework, e.g. [16].

The recent interest in separating codes comes mainly from digital fingerprinting [6]. A vendor distributes digital copies of a copyrighted work, and she wants to prevent the users from making illegal copies. A digital watermark is a perceptually invisible pattern embedded in a digital file. Watermarking can be used to give every sold copy a unique ID, a digital fingerprint, identifying the buyer. If an illegal copy subsequently appears, the user guilty of copying may be identified and prosecuted.

An interesting combinatorial problem arises in the venture to protect against coalitions of pirates. If several users collude, they may compare their copies, and every differing symbol must be part of the fingerprint. Thus having identified part of the fingerprint, the pirates may also change it and produce illegal copies with invalid fingerprint. The fingerprints the pirates are able to forge form the so-called feasible set, defined as

$$F(T) := \{(v_1, \ldots, v_n) \in Q^n \mid \\ \forall i, 1 \le i \le n, \exists (a_1, \ldots, a_n) \in T, a_i = v_i\},$$

where T is the set of fingerprints held by the pirates, Q is the alphabet, and n is the length of a fingerprint.

If the set (code) of valid fingerprints still makes it possible to trace at least one guilty pirate out of a coalition of size t or less, we say that the code has the t-identifiable parent property (t-IPP). If the pirates are able to forge the fingerprint of an innocent user, we say that this user is framed. Codes which prevent framing are called frameproof codes, and this concept coincides with $(t, 1)$-separation. Other kinds of separating codes have also been used to construct IPP codes [4], [3]. It can also be seen that if the code is (t, t)-separating, then no two disjoint pirate coallitions of size at most t can produce the same false fingerprint; and therefore (t, t)-SS are known as t-secure frameproof codes in the fingerprinting literature [24].

In [23] it was proved that the best known asymptotical $(2, 2)$-separating codes are also 2-IPP with ϵ-error. In [22] a new scheme against three pirates is constructed based on separating codes.

The case of $(2, 2)$-separation was introduced by Sagalovich in the context of automata: two such systems transiting simultaneously from state a to a' and from b to b' respectively should be forbidden to pass through a common intermediate state. A state of the system in this case is an n-bit binary string, and the moving from one state to another is obtained by flipping bits one by one. Only shortest paths from the old to the new state are allowed, so moving from a to a' will only involve flipping bits where a and a' differ. The set of valid states Γ forms a $(2, 2)$-separating system, if for any four distinct states, a, a', b, and b' from Γ, the transitions $a \to a'$ and $b \to b'$ cannot pass through any common state. Sagalovich's contribution on this topic is substantial and has been surveyed in [21].

II. Minimum alphabet size for linear SS

If a linear code is to be (t, u)-separating, then the alphabet must have a certain minimum size. Here we give lower bounds on q. The result for binary codes is probably well-known, but the non-binary result appears to be unknown in the literature.

Proposition 1: Let $\mathbf{a}$ and $\mathbf{b}$ be two linearly independent codewords, and write $T = \{\mathbf{a}\} \cup \{\mathbf{b} + \alpha\mathbf{a} \mid \alpha \in \mathsf{GF}(q)\}$. Then $(\mathbf{0}, T)$ is a $(q + 1, 1)$-configuration which is not separated.

Proof: We shall prove that in every position i, at least one codeword in T has a 0. If $a_i = 0$, this holds, so assume $a_i \neq 0$. Then $\mathbf{b} - a_i^{-1} b_i \mathbf{a}$ has 0 in position i, as required. ■

Corrollary 1: If C is q-ary, linear (t, t')-separating, then $\max\{t, t'\} \le q$.

This bound is tight in the binary case, since $(2, 2)$-separating, binary, linear codes are known to exist (e.g. [21]).

First author is with Dept. Informatique et Reseaux, ENST, Paris, France. Email: ⟨cohen@infres.enst.fr⟩.

Second author is with Dept. Informatics, University of Bergen, Norway. Email: ⟨georg@ii.uib.no⟩.

The research was partially supported by the Aurora Programme of the Norwegian Research Council and the Ministère des Affaires Etrangères of France. The second author has also been funded by the Norwegian Research Council under Grant 146874/420.

The work was presented in part at the International Conference on Telecommunications in French Polynesia February 2003.

Theorem 1: If C is a non-binary, linear (t,t')-separating, then $t+t' \leq q+1$.

Proof: We have already proved that $\max\{t,t'\} \leq q$. It only remains to prove that we can construct a non-separated $(t,q+2-t)$-configuration for all t such that $2 \leq t \leq q$. By symmetry, it is sufficient to show this when $t \leq q+2-t$, in particular when $t < q$. Let $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ be all the field elements, where $\alpha_0 = 0$ and $\alpha_1 = 1$. Let $\mathbf{a}$ and $\mathbf{b}$ be two independent codewords. A non-separated $(t,q+2-t)$-configuration is given by

$$(\{\alpha_0\mathbf{a},\ldots,\alpha_{t-1}\mathbf{a}\},\{\alpha_t\mathbf{a},\mathbf{a}+\alpha_1\mathbf{b},\ldots,\mathbf{a}+\alpha_{q+1-t}\mathbf{b}\}).$$

First note that $\alpha_t\mathbf{a}$ matches $\mathbf{0}$ on every position not in $\chi(\mathbf{a})$, and $\mathbf{a}+\mathbf{b}$ matches $\mathbf{a}$ on every position not in $\chi(\mathbf{b})$. In every position in $\chi(\mathbf{a})\cap\chi(\mathbf{b})$, we get t different field values in the first set, and $q+1-t$ different field values from the $\mathbf{a}+\alpha_i\mathbf{b}$. Since there are only q elements in the field, they cannot be separated. ■

III. On $(t,1)$-separating codes

It was proved by Blackburn [5] that any $(t,1)$-separating code has $M \leq t \cdot q^{\lceil n/t \rceil}$. We generalise this result for codes with a guaranteed $(t,1)$-separating weight $\theta_{t,1} = \tau n$. Such codes have been studied in [13], [17] motivated by broadcast encryption.

Partition $\{1,2,..n\}$ into t almost equal parts $P_1,\ldots,P_t$ of size $\lfloor n/t \rfloor$ or $\lceil n/t \rceil$. Say a codeword c is *isolated* on P_i if no other codeword projects onto a n/t-tuple on P_i located at distance less than $(n/t)\tau$ from c.

Lemma 1: If C has $(t,1)$-separating weight $n\tau$ or greater, then every codeword $c \in C$ is isolated on at least one P_i.

Proof: Suppose for a contradiction that there is a codeword $\mathbf{c}_0$ which is isolated on no P_i. Let $\mathbf{c}_i$ be a codeword at distance less than $(n/t)\tau$ from it when projected onto P_i, for $i = 1,\ldots,t$. Now $\mathbf{c}_0$ is separated from $\{\mathbf{c}_1,\ldots,\mathbf{c}_t\}$ on less than $(n/t)\tau$ coordinates per block, or less than $n\tau$ coordinate positions total. This contradicts the assumption on the separating weight τ. ■

Denote by I_i the subset of codewords isolated on P_i. We have just proved that $C \subset \bigcup I_i$. Furthermore, every nonempty I_i is a code of minimum distance at least $\lfloor (n/t)\tau \rfloor$ and thus size at most $q^{\lceil (1-\tau)n/t \rceil}$ by the Singleton bound ([19]). This proves:

Theorem 2: If C has $(t,1)$-separating weight $n\tau$ or greater, then $\#C \leq tq^{\lceil (1-\tau)n/t \rceil}$.

For constant t, this asymptotically gives $R \leq (1-\tau)/t$ when n increases, where $R := (\log_q \#C)/n$ is the code rate. If we let τ tend to zero, we get an upper bound on $(t,1)$-SS, which was found independently in [10] and [5]. The proofs are essentially the same as the one presented here. Asymptotically when n increases, the best possible rate of a $(t,1)$-SS is at most $1/t$.

IV. Upper bounds by projection

In this section, we give a general presentation of the well-known recursive projection arguments for upper bounds. The technique have been used for decades, but the results have continuously been refined in various ways, see e.g. [21]. Here we make yet a step forward in tightening the bounds, both for separating codes and for the related superimposed and completely separating codes.

A. The binary case

Separating codes are related to two stronger concepts. Completely separating codes ((t,t')-CSS) are used in automata theory and fault-tolerant systems alongside the separating codes. Superimposed codes ((t,t')-SI) where introduced in [14], and have been studied in several papers, e.g. [11], [12].

We will consider the binary case only. Consider any $t+t'$ codewords and view them as rows of a matrix. If the code is separating, there must be at least one separating column, which is either $\mathbf{x}_0 = (0\ldots01\ldots1)$ with t zeroes and t' ones, or $\mathbf{x}_1 = (1\ldots10\ldots0)$ with t ones and t' zeroes.

If the code is (t,t')-superimposed, we demand at least one column of type $\mathbf{x}_0$, and if the code is (t,t')-completely separating, we demand both $\mathbf{x}_1$ and $\mathbf{x}_0$. Thus separating codes is clearly the weakest concept, while completely separating systems is the strongest. If $t = t'$, superimposed codes and completely separating codes are equivalent, since the property has to hold for any ordering of the words.

Let $R^{\mathrm{CSS}}(t,t')$, $R^{\mathrm{SI}}(t,t')$, and $R^{\mathrm{SS}}(t,t')$ be the best possible asymptotic rates of (t,t')-CSS, (t,t')-SI, and (t,t')-SS, respectively. Clearly we have

$$R^{\mathrm{SS}}(t,t') \geq R^{\mathrm{SI}}(t,t') \geq R^{\mathrm{CSS}}(t,t') \geq \frac{1}{2}R^{\mathrm{SS}}(t,t').$$

We denote by $\bar{R}^x(t,t')$ any upper bound on $R^x(t,t')$. Let $\bar{R}(\delta)$ be any upper bound on the asymptotic rate of error-correcting codes with normalised minimum distance $\delta = d/n$.

Proposition 2: Any binary (t,u)-separating $(\theta_{0,0},M,\theta_{1,1})$ code Γ with separating weights $\theta_{a,b}$, for $1 \leq a \leq t$ and $1 \leq b \leq u$, gives rise to, for any positive $v < \min\{t,u\}$, a completely $(t-v,u-v)$-separating $(\theta_{v,v},M-2v,2\theta_{v+1,v+1})$ code Γ' with complete-separating weights $\theta'_{a,b} = \theta_{a+v,b+v}$ for $1 \leq a \leq t-v$ and $1 \leq b \leq u-v$.

Proof: Consider two v-tuples V and V' of words from Γ, such that they have separating weight $\theta_{v,v}$. Assume by translation that (V,V') has $\theta_{v,v}$ columns of the form $(0\ldots01\ldots1)$. Let Γ' be the code obtained from Γ by deleting every column where (V,V') is not separated and the $2v$ words from V and V'. Clearly Γ' has the length and size claimed by the proposition. It remains to prove the statement on separating weights.

Let (T,U) be a (t',u')-configuration from Γ where $t' \leq t-v$ and $u' \leq u-v$. Then both $(V\cup T,V'\cup U)$ and $(V'\cup T,V\cup U)$ must have separating weight at least $\theta_{t'+v,u'+v}$, which implies that (T,U) is completely separated with weight at least $\theta_{t'+v,u'+v}$. This holds even when restricting only to the positions where (V,V') is separated. ■

The following proposition is proved in the same way.

Proposition 3: Any completely (t,u)-separating $(n,M,2\theta_{1,1})$ code with completely separating weights $\theta_{a,b}$, for $1 \leq a \leq t$ and $1 \leq b \leq u$, gives rise to, for any positive $v < \min\{t,u\}$, a completely $(t-v,u-v)$-separating

(t, t')	CSS	SIC	SS
$(2, 1)$	—	0.3219[2]	0.5[1]
$(3, 1)$	—	0.1993[2]	0.3333[1]
$(3, 2)$	0.06627	0.07449[3]	0.1202
$(4, 2)$	0.04301	0.04552[3]	0.07994
$(4, 3)$	0.01533	0.01828[3]	0.02951

(t, t)	CSS	SS
$(1, 1)$	1.0000	1.0000
$(2, 2)$	0.1610[2]	0.2835[4]
$(3, 3)$	0.03534	0.06627[5]
$(4, 4)$	0.008368	0.01630
$(5, 5)$	0.002042	0.004037

[1] Theorem 2
[2] [12]
[3] [15]
[4] Well known, see [21].
[5] A slightly stronger bound is alleged in [8].

TABLE I

UPPER BOUNDS ON COMPLETELY SEPARATING CODES (CSS), SUPERIMPOSED CODES (SIC), AND SEPARATING CODES (SS) OVER A BINARY ALPHABET.

$(\theta_{v,v}, M - 2v, 2\theta_{v+1,v+1})$ code with complete-separating weights $\theta'_{a,b} = \theta_{a+v,u+v}$ for $1 \le a \le t-v$ and $1 \le b \le u-v$.

Theorem 3: We have for $t, u \ge 2$ that

$$R^{\mathrm{CSS}}(t,u) \le \bar{R}\left(\frac{2R^{\mathrm{CSS}}(t,u)}{\bar{R}^{\mathrm{CSS}}(t-1,u-1)}\right),$$

$$R^{\mathrm{SS}}(t,u) \le \bar{R}\left(\frac{R^{\mathrm{SS}}(t,u)}{\bar{R}^{\mathrm{CSS}}(t-1,u-1)}\right).$$

Proof: Let C be a (t,u)-CSS with rate $R = R^{\mathrm{CSS}}(t,u)$, and let C' be the $(t-1,u-1)$-CSS which exists by Proposition 3. Denote by R' the rate of C'. We have that

$$\delta = 2\frac{\theta_{1,1}}{\theta_{0,0}} = 2\frac{\log M}{\theta_{0,0}}\frac{\theta_{1,1}}{\log M} = 2R/R'.$$

Now, obviously $R \le \bar{R}(\delta)$, which is decreasing in δ_t, and this gives the result. The bound on R^{SS} is similar, except that the minimum distance of C is $d = \theta_{1,1}$ instead of $2\theta_{1,1}$. ■

This theorem provides a recursive bound on separating codes. The general idea is not new, at least the derived bound on $(2,2)$-SS has been known for ages, see [21]. Even so, the results we obtain here for (t,t)-CSS are stronger than those recently presented in [12] (except for $t = 2$).

We use the linear programming bound for $\bar{R}(\delta)$, as given in the following theorem in its q-ary version. See [2] for the non-binary form and [20] for the original (binary) version. Also note improvements in [1], [18].

Theorem 4 (Linear Programming Bound): For any (n, M, d) q-ary code, we have

$$R(\delta) \le H_q(((q-1) - (q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)})/q),$$

where

$$H_q(x) = -(1-x)\log_q(1-x) - x\log_q x + x\log_q(q-1).$$

In Table I, we summarise the rate we get for small t and t', and $q = 2$. Most of the rates are obtained by using the theorems of this section recursively. The first bounds in the iterations are copied from other works. Observe that we improve the bounds also on (t,t)-superimposed codes for $t \ge 3$.

Example 1: Let C_1 be an asymptotic class of $(\theta_0, 2^k, \theta_1)$ $(3,3)$-SS. Then there is an asymptotic class C_2 of $(\theta_1, 2^k, \theta_2)$ $(2,2)$-CSS. We have that $R_2 = k/\theta_1 \le 0.161$, and

$$R_1 = k/\theta_0 = R_2\delta_1 \le 0.161\delta_1,$$

which is equivalent to

$$\delta_1 \ge R_1/0.161.$$

We can use any upper bound $\bar{R}(\delta)$ on R_1, and get

$$R_1 \le \bar{R}(\delta_1) \le \bar{R}(R_1/0.161).$$

Using the Theorem 4, we get $R_1 \le 0.0663$.

B. The ternary case

In the non-binary case, complete separation is not clearly defined. When $q > 3$, we are not able to prove a recursive bound stronger than

$$R_q^{\mathrm{SS}}(t,u) \le \bar{R}\left(\frac{R_q^{\mathrm{SS}}(t,u)}{\bar{R}_q^{\mathrm{SS}}(t-1,u-1)}\right),$$

which is considerably weaker than the binary result. The reason for this is found in the proofs of Propositions 2 and 3: since there are four alphabet symbols (or more), it is possible to have one column which separates both $(V \cup T, V' \cup U)$ and $(V' \cup T, V \cup U)$.

In the ternary case, though, we get a strong analogue of the binary results by defining ternary pseudo-completely separating weights. Let (T, U) be a (t,u)-configuration. A separating column i is of Type 0 if $x_i \ne 1$ for all $\mathbf{x} \in T$ and $y_i \ne 0$ for all $\mathbf{y} \in U$. It is of Type 1 if $x_i \ne 0$ for all $\mathbf{x} \in T$ and $y_i \ne 1$ for all $\mathbf{y} \in U$. Note that one column can be both of Type 0 and of Type 1 if and only if $q > 3$.

The pseudo-completely separating weight of a ternary code C is the largest number $\theta_{t,u}$ such that any (t,u)-configuration has at least $\theta_{t,u}$ separating columns of Type 0 and at least $\theta_{t,u}$ separating columns of Type 1.

The following two lemmata can be proved using the proof of Proposition 2.

Lemma 2: Any ternary (t,u)-separating $(\theta_{0,0}, M, \theta_{1,1})$ code Γ with separating weights $\theta_{a,b}$, for $1 \le a \le t$ and $1 \le b \le u$, gives rise to, for any positive $v < \min\{t,u\}$, a pseudo-completely $(t-v, u-v)$-separating $(\theta_{v,v}, M-2v, 2\theta_{v+1,v+1})$ code Γ' with pseudo-completely separating weights $\theta'_{a,b} = \theta_{a+v,u+v}$.

Lemma 3: Any ternary pseudo-completely (t,u)-separating $(\theta_{0,0}, M, 2\theta_{1,1})$ code Γ with pseudo-completely separating weights $\theta_{a,b}$, for $1 \le a \le t$ and $1 \le b \le u$, gives rise to, for any positive $v < \min\{t,u\}$, a pseudo-completely $(t-v, u-v)$-separating $(\theta_{v,v}, M-2v, 2\theta_{v+1,v+1})$ code Γ' with pseudo-completely separating weights $\theta'_{a,b} = \theta_{a+v,u+v}$.

Analogously to Theorem 3, we get the following theorem. Table II follows by combining Theorem 5 with the linear programming bound.

(t,t)	PCSS	SS
$(1,1)$	1	1
$(2,2)$	0.2197	0.3537
$(3,3)$	0.06204	0.1138
$(4,4)$	0.01913	0.03675
$(5,5)$	0.006120	0.01202

(t,t')	PCSS	SS
$(3,2)$	0.1268	0.2197
$(4,3)$	0.03751	0.07056
$(5,4)$	0.01180	0.02290
$(4,2)$	0.08978	0.1605
$(5,3)$	0.02713	0.05167
$(5,2)$	0.06966	0.1268

TABLE II

Upper bounds on ternary separating codes, computed by using the bound $R \leq 1/t$ for $(t,1)$-SS and -PCSS (Theorem 2) and recursive application of Theorem 5.

$t+u$	Rate
3	0.3537
4	0.1683
5	0.09050
6	0.05206

TABLE III

Upper bounds on ternary linear separating codes, computed by recursive application of Corollary 2.

Theorem 5: We have for $t, u \geq 2$ that

$$R_3^{\mathrm{PCSS}}(t,u) \leq \bar{R}\left(\frac{2R_3^{\mathrm{PCSS}}(t,u)}{\bar{R}_3^{\mathrm{PCSS}}(t-1,u-1)}\right),$$

$$R_3^{\mathrm{SS}}(t,u) \leq \bar{R}\left(\frac{R_3^{\mathrm{SS}}(t,u)}{\bar{R}_3^{\mathrm{PCSS}}(t-1,u-1)}\right).$$

C. The linear case

Let $R_q^{\mathrm{LSS}}(t,u)$ be the highest possible rate for an asymptotic family of linear, q-ary (t,u)-separating code.

Proposition 4: Any linear separating $[\theta_{0,0}, k, \theta_{1,1}]$ code C with separating weights $\theta_{a,b}$, where $1 \leq a \leq t$ and $1 \leq b \leq u$, gives rise to a linear separating $[\theta_{0,1}, k-1, \theta_{1,2}]$ code C' with separating weights $\theta'_{a,b} = \theta_{a,b+1}$, where $1 \leq a \leq t$ and $1 \leq b \leq u-1$.

Proof: Let $\mathbf{c} \in C$ be a codeword of weight $\theta_{1,1}$. Let C' be the code obtained by shortening C on every position where $\mathbf{c}$ is zero. It remains to prove that $\theta_{a,b}(C') \geq \theta_{a,b+1}(C)$ for all a and b. It is sufficient that any (a,b)-configuration (A,B) of C' with $\mathbf{0} \in A$ has separating weight at least $\theta_{a,b+1}(C)$. Consider the corresponding $(a,b+1)$-configuration $(A,B') = (A, B \cup \{\mathbf{c}\})$ in C. Observe that (A,B') can only be separated where $\mathbf{c}$ is non-zero, i.e. on positions existing in C'. Hence $\theta(A,B) = \theta(A,B') \geq \theta_{a,b+1}(C)$ as required. ■

Corrollary 2: For any $t \geq 1$ and $u \geq 2$, we have

$$R_q^{\mathrm{LSS}}(t,u) \leq \bar{R}\left(\frac{R_q^{\mathrm{LSS}}(t,u)}{\bar{R}_q^{\mathrm{LSS}}(t,u-1)}\right).$$

Note that this bound depends only on the sum $t+u$. We have computed numerical values for $q=3$ in Table III. Applying the corollary for $q=2$ gives the same bounds as the ones obtained from intersecting codes in [9].

V. Conclusion

We have refined the upper bounds on (t,u)-separating codes. This has also led to improvements on the upper bounds for (t,t)-superimposed codes (completely separating codes).

References

[1] M. Aaltonen, “A new upper bound on nonbinary block codes,” *Discrete Math.*, vol. 83, no. 2-3, pp. 139–160, 1990.

[2] M. J. Aaltonen, “Linear programming bounds for tree codes,” *IEEE Trans. Inform. Theory*, vol. 25, no. 1, pp. 85–90, 1979.

[3] A. Barg, G. R. Blakley, and G. A. Kabatiansky, “Digital fingerprinting codes: Problem statements, constructions, identification of traitors,” *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 852–865, Apr. 2003.

[4] A. Barg, G. Cohen, S. Encheva, G. Kabatiansky, and G. Zémor, “A hypergraph approach to the identifying parent property,” *SIAM J. Disc. Math.*, vol. 14, no. 3, pp. 423–431, 2001.

[5] S. R. Blackburn, “Frameproof codes,” *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499–510, 2003.

[6] D. Boneh and J. Shaw, “Collusion-secure fingerprinting for digital data,” *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897–1905, 1998, presented in part at CRYPTO’95.

[7] B. Chor, A. Fiat, and M. Naor, “Tracing traitors,” in *Advances in Cryptology - CRYPTO ’94*, ser. Springer Lecture Notes in Computer Science, vol. 839. Springer-Verlag, 1994, pp. 257–270.

[8] F. Chung, R. Graham, and T. Leighton, “Guessing secrets,” *Electron. J. Combin.*, vol. 8, 2001.

[9] G. D. Cohen, S. B. Encheva, S. Litsyn, and H. G. Schaathun, “Intersecting codes and separating codes,” *Discrete Applied Mathematics*, vol. 128, no. 1, pp. 75–83, 2003.

[10] G. D. Cohen and H. G. Schaathun, “New upper bounds on separating codes,” in *2003 International Conference on Telecommunications*, Feb. 2003.

[11] A. G. D′yachkov and V. V. Rykov, “A survey of superimposed code theory,” *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, vol. 12, no. 4, pp. 229–242, 1983, english translation from Russian.

[12] A. G. D′yachkov, P. Vilenkin, A. Macula, and D. Torney, “Families of finite sets in which no intersection of ℓ sets is covered by the union of s others,” *J. Combin. Theory*, vol. 99, pp. 195–208, 2002.

[13] J. Garay, J. Staddon, and A. Wool, “Long-lived broadcast encryption,” in *Crypto 2000*, ser. Springer Lecture Notes in Computer Science, vol. 1880, 2000, pp. 333–352.

[14] W. Kautz and R. Singleton, “Nonrandom binary superimposed codes,” *IEEE Trans. Inform. Theory*, vol. 10, no. 4, pp. 363–377, Oct. 1964. [Online]. Available: http://ieeexplore.ieee.org/iel5/18/22624/01053689.pdf

[15] H. K. Kim, V. Lebedev, and D. Y. Oh, “Some new results on (w,r) superimposed codes,” 2003, preprint.

[16] J. Körner and G. Simonyi, “Separating partition systems and locally different sequences,” *SIAM J. Discrete Math.*, vol. 1, pp. 355–359, 1988.

[17] R. Kumar, S. Rajagopalan, and A. Sahai, “Coding constructions for blacklisting problems without computational assumptions,” in *Crypto’99*, ser. Springer Lecture Notes in Computer Science, vol. 1666, 1999, pp. 609–623.

[18] T. Laihonen and S. Litsyn, “On upper bounds for minimum distance and covering radius of non-binary codes,” *Designs, Codes, and Cryptography*, vol. 14, no. 1, pp. 71–80, 1998.

[19] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, 1977.

[20] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, “New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities,” *IEEE Trans. Inform. Theory*, vol. IT-23, no. 2, pp. 157–166, 1977.

[21] Y. L. Sagalovich, “Separating systems,” *Problems of Information Transmission*, vol. 30, no. 2, pp. 105–123, 1994.

[22] H. G. Schaathun, “Fighting three pirates with scattering codes,” 2003, submitted to ISIT’04 in Chicago.

[23] ——, “Fighting two pirates,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Springer Lecture Notes in Computer Science, vol. 2643. Springer-Verlag, May 2003, pp. 71–78.

[24] J. N. Staddon, D. R. Stinson, and R. Wei, “Combinatorial properties of frameproof and traceability codes,” *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1042–1049, 2001.